

AD-A168 861

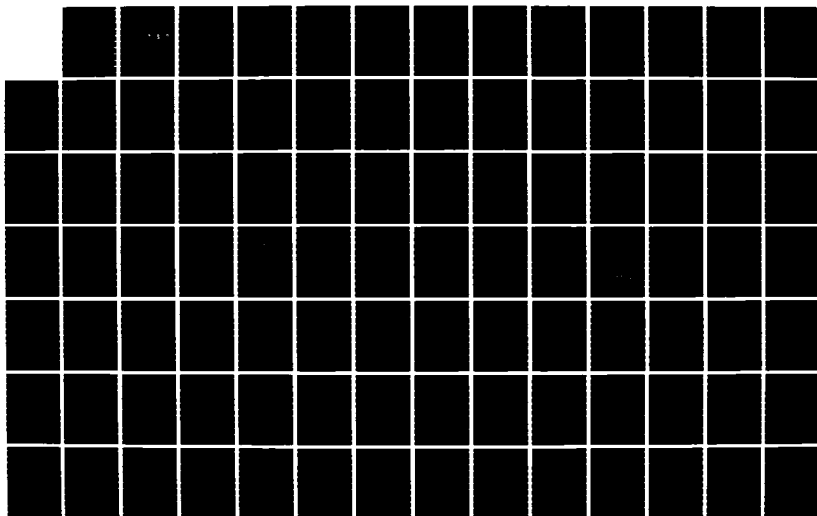
LOCAL AREA NETWORK STANDARDS AND GUIDELINES FOR US
MARINE CORPS APPLICATIONS(U) NAVAL POSTGRADUATE SCHOOL
MONTEREY CA T J HINES 27 MAR 86

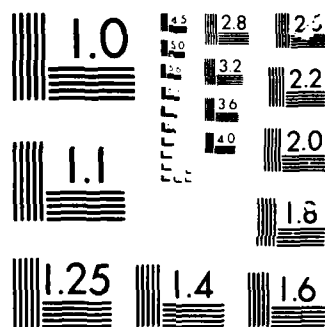
1/2

UNCLASSIFIED

F/G 17/2

NL



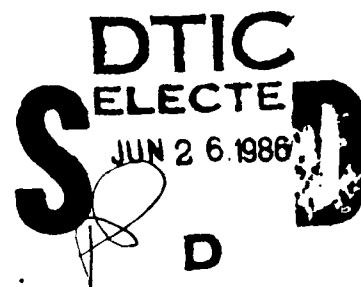


AD-A168 861

DTIC FILE COPY

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

LOCAL AREA NETWORK STANDARDS AND GUIDELINES
FOR U.S. MARINE CORPS APPLICATIONS

by

Timothy J. Hines

March 1986

Thesis Advisor:

Jack W. Lapatra

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED			1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY			3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.		
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE					
4. PERFORMING ORGANIZATION REPORT NUMBER(S)			5. MONITORING ORGANIZATION REPORT NUMBER(S)		
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b. OFFICE SYMBOL (If applicable) Code 62	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School			
6c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000			
8a. NAME OF FUNDING / SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER			
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS			
		PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO
11. TITLE (Include Security Classification) LOCAL AREA NETWORK STANDARDS AND GUIDELINES FOR U.S. MARINE CORPS APPLICATIONS					
12. PERSONAL AUTHOR(S) Himes, Timothy J.					
13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day) 1986 March 27	15. PAGE COUNT 122		
16. SUPPLEMENTARY NOTATION					
17. COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB-GROUP	local area network; LAN; media; topologies; standards; access methods; protocols; network management; specification strategy; documentation; (MCDM) Marine Corps Data Network		
19. ABSTRACT (Continue on reverse if necessary and identify by block number) This thesis highlights the need for specific guidance and standards in the U.S. Marine Corps local area network (LAN) specification and selection process. Media, topologies, components access methods, protocols, standards and other technologies are used to characterize the current technical environment. A strategy for LAN specification and selection is presented. This strategy stresses top-down, user requirement, protocol performance oriented techniques vice the bottom-up, technical design selection oriented techniques in use today. Thorough documentation of user requirements, higher-level services, higher-level protocols, and an information and networking strategy along with other considerations like facilities/support, expected general performance, network management, and security is the method proposed for preparation of a complete specification document. A centrally coordinated U.S. Marine Corps specification and design database is also proposed to ensure future interoperability, connectivity, and support.					
20. DISTRIBUTION / AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT <input type="checkbox"/> DTIC USERS			21. ABSTRACT SECURITY CLASSIFICATION unclassified		
22a. NAME OF RESPONSIBLE INDIVIDUAL Jack W. LaPatra			22b. TELEPHONE (Include Area Code) (408) 646-2249	22c. OFFICE SYMBOL 54LP	

Approved for public release; distribution is unlimited.

Local Area Network
Standards and Guidelines for
U.S. Marine Corps Applications

by

Timothy J. Himes
Major, United States Marine Corps
B.A., Walsh College, 1969

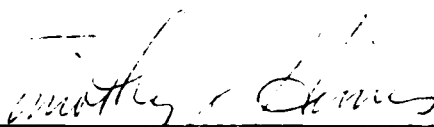
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEM MANAGEMENT


from the

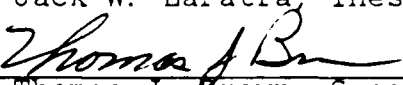
NAVAL POSTGRADUATE SCHOOL
March 1986

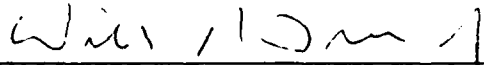
Author:

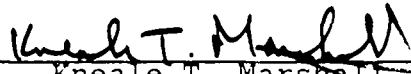

Timothy J. Himes

Approved by:


Jack W. LaPatra, Thesis Advisor


Thomas J. Brown, Second Reader


Willis R. Greer Jr., Chairman,
Department of Administrative Sciences


Kneale T. Marshall
Dean of Information and Policy Sciences

ABSTRACT

This thesis highlights the need for specific guidance and standards in the U.S. Marine Corps local area network (LAN) specification and selection process. Media, topologies, components, access methods, protocols, standards and other technologies are used to characterize the current technical environment. A strategy for LAN specification and selection is presented. This strategy stresses top-down, user requirement, protocol performance oriented techniques vice the bottom-up, technical design selection oriented techniques in use today. Thorough documentation of user requirements, higher-level services, higher-level protocols, and an information and networking strategy along with other considerations like facilities/support, expected general performance, network management, and security is the method proposed for preparation of a complete specification document. A centrally coordinated U.S. Marine Corps specification and design database is also proposed to ensure future interoperability, connectivity, and support.

Accession For	
NTIS CRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	

TABLE OF CONTENTS

I.	INTRODUCTION	8
A.	GENERAL	8
B.	THE PROBLEM	12
II.	BASIC LOCAL AREA NETWORKS	16
A.	A DEFINITION	16
B.	MEDIA	17
	1. Twisted-Pair Cable	18
	2. Coaxial Cable	19
	3. Fiber Optics	21
	4. Other Media	23
C.	TOPOLOGIES	23
	1. Star	23
	2. Ring	26
	3. Bus/Tree	27
D.	ACCESS METHODS	29
	1. Time Division Multiple Access (TDMA)	30
	2. Carrier Sense Multiple Access (CSMA)	30
	3. Token Passing	31
E.	PROTOCOLS AND STANDARDS	32
	1. General	32
	2. The OSI Model	33
	3. LAN Standards	37
	4. High Layer Protocol Standards	40
F.	PBX TECHNOLOGY	43
III.	A STRATEGY FOR LAN SPECIFICATION	47
A.	GENERAL	47
B.	USER REQUIREMENTS	49
C.	HIGHER-LEVEL SERVICES	55

D.	HIGHER-LEVEL PROTOCOLS	59
E.	INTERCONNECTION REQUIREMENTS	66
	1. Local Network Interconnection	66
	2. Local/Long Distance Network Interconnection	69
	3. USMC Local/Long Distance Network Strategy	78
F.	LAN SPECIFICATIONS	89
	1. General	89
	2. Performance	91
	3. Facilities/Support	95
	4. Network Management	98
	5. Security	99
G.	SUMMARY	103
IV.	A LAN SELECTION STRATEGY	104
	A. GENERAL	104
	B. USER/DEVELOPER EXPERIENCE	106
	C. THE SINGLE SPECIFICATION APPROACH	108
V.	SUMMARY/CONCLUSIONS	115
	APPENDIX : ACRONYMS	122
	LIST OF REFERENCES	125
	INITIAL DISTRIBUTION LIST	127

LIST OF TABLES

I	LAN MEDIA COMPARISON	24
II	MESSAGE AND DOCUMENT HANDLING SUBFUNCTIONS . . .	56
III	SUMMARY OF ASSOCIATION OF SERVICES WITH THE OSI REFERENCE MODEL	61
IV	COMMUNICATIONS MODEL CHECKLIST GENERIC SERVICES AND SUBFUNCTIONS	62
V	APPLICATIONS LAYER CHECKLIST	63
VI	ADDRESS MANAGEMENT	64
VII	MCDN DESIGNATIONS	81
VIII	MCDN SUBAREA ASSIGNMENTS	82
IX	NODE ID, DESTINATION ID, AND LINE NUMBER	83
X	RECOMMENDED LAN SPECIFICATIONS FROM MARCH 1985 RASC CAMP PENDLETON LAN TEST	109

LIST OF FIGURES

2.1	Mesh Topology	25
2.2	Star Topology	25
2.3	Ring Topology	27
2.4	Bus Topology	28
2.5	Tree Topology	29
2.6	ISO Open System Interconnection Reference Model (OSI/RM)	35
2.7	Relationship Between OSI/RM and LAN Standards . . .	39
2.8	OSI/DOD INTERNET Comparison	44
3.1	LAN Specification: Where to Begin?	48
3.2	LAN Specification/Selection Strategy	50
3.3	Protocol Layer Encapsulation	66
3.4	LANs Interconnected by a Bridge	70
3.5	Communication Protocol Architecture Comparison . .	74
3.6	DNA Protocol Architecture	76
3.7	SNA Protocol Architecture	78
3.8	Marine Corps Data Network (MCDN)	80
3.9	Phase II MCDN/DDN IPR	86
3.10	Phase III MCDN/DDN IPR	87
3.11	Local Networks Connected Through MCDN Hosts and DDN	89
3.12	Local Networks Connected Through MCDN Hosts and Network	90
3.13	Local Networks With Distributed Processing Connected Through DDN	91
3.14	Local Networks With Distributed Processing Connected Through DDN and Public PSN	92
3.15	Network Management Services	100
4.1	ULANA Frequency Allocation	112
4.2	Broadband Distribution System for ULANA	113

I. INTRODUCTION

A. GENERAL

The world around us is undergoing a great deal of change driven by the increased use of electronics, especially computers. Our whole working environment is being populated by increasingly complex systems, all of which seem to be computer controlled. These computers, regardless of their scale, are nothing more than data processing devices; raw data is fed in, a program controlled process acts on the data, and the processed data is then output in the form of usable information. The evolution in computer configuration and usage over the past 20-30 years caused a veritable information explosion. This explosion was not only a result of increased computer processing capability but also the ability to place this processing capability on an individual user's desk.

The early centralized processing techniques involved simple two wire configurations from card readers to central processing units (CPU) and from the CPU to a printer. Individual jobs were dropped at the computer center window and picked up later after processing. Simple equipment configurations were easy to troubleshoot and maintain. Things got a little more complicated with the addition of data communications between plotters, remote printers and other devices directly connected to the CPU. However, all equipment was still within one common controlled area where maintenance remained easy but wiring increased in complexity. Terminal processing came next and along with it the problem of allocating an individual wire pair connection for each machine; computer networking in its most basic form was born. Initially handled by locating all the terminals in a room close to the CPU, data communications experienced

the first significant breakthrough in the early 1960's when users began to separate from their central computer systems. The concept of time shared systems with multiple users at different physical locations became reality.

In the early 1970's, network complexity increased when coaxial cable and communications devices like multi-drop lines, multiplexors, concentrators, and intelligent terminal devices were used to enhance and extend communications between users and the CPU. As the number of users increased so did the communications overhead as well as the competition for time at the central processing unit. The growing network of cables and networking equipment increased the maintenance burden. Special computers were developed to remove the communications burden from the CPU and CPUs themselves were made faster and more powerful. However, these improvements could not keep up with the increased user demand.

The intelligent terminal was probably most instrumental in the move away from large, costly, centralized mainframe processing systems. A sharp decrease in size and cost of computers accompanied by specially designed functional software packages freed users from dependence on the central computing system. It also gave them the opportunity to acquire powerful personal computing devices in large numbers. Micro-computers emerged as personal productivity tools. International Data Corporation's most recent estimates on computer shipments indicate 1986 U.S. desktop personal computer (PC) shipments totalling \$14.2 billion will exceed the \$13.7 billion expenditure estimates for mainframe systems [Ref. 1: p. 35].

In terms of cost-savings and processing performance, use of personal computers has many advantages over the traditional time sharing approach. Higher worker productivity, better computer accessibility and availability, faster

responsiveness, greater interaction, and a wider choice of equipment are all advantages of the new PC technology. Software such as spreadsheets, database managers, wordprocessors, etc, all help individual users produce higher quality work easier and faster. However, along with these advantages come new problems. Expensive peripheral devices (printers, mass storage, etc,), connected to the central processing facility and so long taken for granted, were now needed at each individual workstation. The integrity of data files previously maintained in a common database was quickly compromised by individual updates performed at different times and in different ways at each workstation. Sharing data went from simple file access on the mainframe to hand carried discs from workstation to workstation or repeated manual database generation and maintenance at each station. Huge mainframe program libraries, previously centrally maintained and accessible by all users, now had to be reproduced and provided to each individual user (if his PC had the memory capability to use them). It became obvious that using the PC as a standalone device tapped only a fraction of its potential not to mention the disadvantages caused by separation from a central processing and control point. Cost effective ways of linking these disparate sources of information processing and storage was viewed as the next logical step toward increasing productivity through automation.

Linking individual stations to host computers via modems and standard telephone lines was the communication and computer industry's first attempt at solving this networking problem. However, the speed limitations(usually less than 1200 bits per second (bps)) and the dependence on a host computer for connection to other users made this technique an inefficient communications solution. Local area networks (LAN) are now emerging as the logical evolutionary step in

development of a shared multi-user network. Although distinctly different from the traditional time-shared processor systems, LAN technology is quickly approaching the capabilities and applications of centralized mainframe time-sharing systems.

LANs have been around since the middle 1970's when Datapoint Corp. introduced its first version. This new networking technique promised to provide a flexible way to link computers, terminals, printers, memories, etc, so they could exchange data at high speeds [Ref. 2: p. 140]. Since then the number of manufacturers of local networks or local network products has grown to over 200. [Ref. 3: p. 124]. These vendors offer a wide variety of topologies, control structures, media, access control techniques, and other items supposedly designed to suit the prospective buyer's individual needs. They offer the potential for more flexible connectivity among processors, workstations, storage devices, and expensive peripherals in the local area. These features are available at greater speeds and lower cost than possible in the previous host-dependent data processing environment. This proliferation of vendors has generated many innovative and useful approaches to the networking solution. However, the differences in these approaches has caused a great deal of confusion on the part of prospective buyers. They have also caused the procurement and installation of many heterogeneous networks that can't support the same kind of equipment and can't intercommunicate.

In many ways, LAN technology is still in its infancy. Most vendors today provide a transmission medium with low level protocols either compatible with other products they produce or specially designed to suit a specific user community. Some have attempted to adopt "open systems" capable of connecting a wide variety of user equipment. None, however, have a design that will soon become the standard or

clear cut solution to everyone's needs. Protocol layered networking architectures like the Open Systems Interconnection Reference Model (OSI/RM) of the International Standards Organization (ISO) provide a general structure of protocol definition [Ref. 4: p. 2-3]. The painfully slow process of high level protocol standards development from sources like the Institute of Electrical and Electronics Engineers (IEEE) Computer Society has resulted in the adoption of several "defacto" standards by developers who hope they will be officially sanctioned at some point in the future. Many buyers think that they will simply go out and buy the latest technology only to discover that the advertised compatibility is only at the physical and link layer of the ISO OSI model. Higher-level protocols that allow intermachine and inter-LAN communications are not yet supported.

B. THE PROBLEM

Many organizations within the U.S. Marine Corps are looking for ways to improve their personal productivity and information sharing capabilities. The need for data communications connectivity, particularly among personal computers and office automation equipment, is growing daily. The current Marine Corps Data Network (MCDN), which is based on IBM's System Network Architecture (SNA) and pre-SNA architectures, cannot totally and efficiently meet the needs of these new asynchronous devices. LANs are the most often mentioned solution to this problem but no official guidance on LAN standards has been published. It is very difficult to develop the thorough specifications needed to define requirements and solicit vendor solutions using only the confusing and inflated manufacturer advertisements. Although applications should drive network design, many "system hunters" find themselves developing broad or superficial requirements then comparing and evaluating the

capabilities of existing hardware and software solutions to satisfy these requirements. As a result, thorough definition of user needs is never accomplished.

Initially, purchase of individual productivity tools such as office automation products and individual intelligent workstations (PCs) was basically decentralized. The wide variety of vendor products permitted wide variations in capabilities. The cost for these tools was not particularly high and organizations basically used them to improve productivity within their own span of control. This had little affect on other organizations. Now these productivity tools are moving from low cost, individual, equipment elements to costly, sophisticated, equipment networks designed to increase productivity through information sharing and reduce expenses by sharing use of high cost peripheral devices. The cost of special cables, interface devices, and sophisticated servers along with individually purchased maintenance and support contracts are rapidly off-setting the advantages of low cost individual workstations over the traditional mainframes approach. The specification and selection of these networks deserves more detailed consideration and guidance than broadly specified user requirements augmented by technical specifications detailing vendor strategies that already exist.

The current LAN procurement process seems to be an extension of the PC procurement process aimed primarily at solving a local need. There is little or no immediate concern for standardization of applications and communications procedures to facilitate future connectivity. If a new telephone switchboard came along which dramatically improved local telephone switching performance for a base or unit but reduced the ability to exchange information on long distance AUTOVON and commercial networks with that base or unit, would we permit its purchase? Permitting LAN

procurements to concentrate only on local individual unit or base needs and applications may lead to serious interoperability and growth problems in the future. Interface parameters for inter-LAN communications as well as existing and evolving wide area networks (WAN) should be considered in all LAN procurements. What about connectivity via alternative, available, less costly means? Digital PBX's, CATV systems, and scheduled coaxial and fiber optic upgrades to existing base cable plants are often overlooked as potential substitutes for sophisticated and costly individual LAN connection and transmission systems. Will future voice, data, imagery, and video requirements be satisfied by highly centralized super computers and integrated voice and data computerized telephone exchanges; by distributed voice over data local area networks with sophisticated servers, bridges for inter LAN communications and gateways to mainframes and long distance integrated voice and data networks; or by some other combination of these maturing advanced technologies?

This thesis highlights the need for specific guidance and if possible Marine Corps wide standards in the LAN specification and selection process by detailing the many technical and logical performance issues that must be addressed when 1) trying to make near-term individual system design decisions and 2) attempting to shape the long-term evolution toward a more effectively integrated network design. Media, topologies, components, access methods, protocols, standards and other technologies are discussed in an attempt to characterize the current technical environment. A strategy for LAN specification and selection is presented. This strategy stresses top-down, user requirement, protocol performance oriented techniques vice the bottom-up technical design selection oriented techniques in use today. User requirements, higher-level services, higher-level protocols, and an information and networking strategy are used to determine

whether a LAN is the appropriate technology. If properly prepared, LAN specifications directly translated from user requirements plus other considerations like facilities/support, expected general performance, network management, security and others will result in vendor proposals that address needed functional requirements vice concentration on their own system features and functions. A centrally coordinated LAN specification and design process is needed to ensure future interoperability and connectivity.

II. BASIC LOCAL AREA NETWORKS

A. A DEFINITION

As the name implies, a local network is a relatively short-distance, high-speed scheme for connecting various computing resources. The distances covered by these networks depend on the products used and generally range from a few hundred yards to 30 miles. Using the word "local" in the name was probably done to contrast this networking technique with long-haul telephone and data switching networks.

More technically defined, a local area network is a data telecommunications system designed to network a number of independent devices like personal computers, printers, mass storage devices, plotters, host computers, terminals, television cameras, television receivers, sensing equipment, and telephones. They are usually owned by a single organization, restricted to small geographic areas (a building or group of buildings), and use moderate to high data rates (1 to 10 million bits per second) [Ref. 5: p. 15]. They are normally subsystems of larger information processing systems used to provide data transport, switching, and network management functions. Many support a wide variety of applications like file editing and transfer, graphics, word processing, electronic mail, database management, high speed video, and digital voice.

Most LANs use a packet transmission technique to break messages into shorter segments, each with an originating and destination address code. The network itself consists of some form of communications medium (cable) of limited length to carry transmissions plus interface units to connect all devices served by the network. Some permit only the supplier's terminals and processors to be connected while others

permit any manufacturer's equipment to be connected. Depending on the access scheme used to control the medium, each station transmits in an assigned time slot, an assigned order, or when it can seize control of the medium by competing with other stations. The user normally purchases the cabling and interface units, then installs and maintains them himself or arranges for installation and maintenance by the supplier. Before looking at a strategy for specifying and selecting a LAN, an introduction to the major technical features and functions currently available is in order.

B. MEDIA

The transmission medium is the physical connection between components in the network. There are several forms of transmission media used in LAN configurations and all have earned the right to be considered due to their respective advantages and disadvantages. Among the most familiar choices are twisted-pair wire, coaxial cable, and fiber optic cable.

Selecting the appropriate medium is often a critical decision when designing a computer communications network. Generally, technology, bandwidth, connectivity and distance along with applications and cost are the characteristics used to compare the different media choices. These factors enable the designer and prospective buyer to evaluate each medium in terms of performance features like reliability, simplicity, speed, and noise immunity as well as ease of installation, maintenance, and reconfiguration.

Most signals cannot be sent in their original form, so some sort of modulation or encoding technique is required before transmission. Both analog and digital transmission methods, each of which has its own unique properties, are used to propagate signals on the various media. Since both methods can be affected by attenuation and/or distortion during transmission due to the physical properties of each

medium, other components designed to offset these noise problems must be considered. Amplifiers, repeaters, and equalizers are often used to compensate for signal losses or to restore distorted waveforms to their original shape.

The signaling speed capability on the media is often measured in the width of the signal spectrum it can handle or more appropriately, its bandwidth. The faster the signal can change with respect to time, the faster the signal speed; normally measured in bits per second (bps). Higher signal speeds require more bandwidth for transmission.

1. Twisted-Pair Cable

A twisted-wire network is just what the name implies: a network of twisted wires with two or more wires connecting each remote device in a point-to-point fashion with a central switching or processing node. The wires, normally made of copper, have a thin insulation coating and are arranged in a regular geometric pattern (parallel or spiral) to reduce noise and ensure that the electrical properties are constant throughout the length of the line. Both analog and digital signals can be passed in twisted-pair but due to its limited bandwidth characteristics, relatively slow signal speeds are achievable. If analog signals are used, modems are required at both ends to first modulate the incoming digital information into analog form, transmit it over the twisted-pair, and demodulate the signal back to its original digital form at the destination. This process, which produces relatively slow speeds of 300-9600 bps on a normal 3 KHz voice channel, is most commonly used for data transmissions through Private Automatic Branch Exchange (PABX) telephone switching systems designed to handle analog voice telephone calls. Recent advances in Computerized Branch Exchange (CBX) telephone systems which employ digital transmission techniques have allowed speeds as high as 64,000 bps to be achieved on local loops. In these systems,

analog voice signals are converted to digital signals using pulse code modulation (PCM) techniques for digital transmission while the digital data signals are already in a form suitable for transmission and switching.

Twisted pair is often the least expensive per foot to install over short distances. However, when additional costs for line conditioning or coding equipment used to extend the range and speed is added to the cost of the wire, overall installation costs approach that of other media like coaxial cable. This media (using analog transmission via modems) provides the transmission backbone and in some cases the terminal interface for MCDN.

2. Coaxial Cable

Coaxial cable, like twisted pair, has two conductors but it is constructed differently to permit operation over a wider range of frequencies. It consists of a flexible conductive cylinder (shell) with an inner conductor in the center. The space between the cylinder and the inner conductor is filled with an insulator to maintain isolation between the conductors. The insulator can be a solid dielectric material or air with dielectric supports an inch apart to separate the conductors. The entire cable is then encased in an outer insulative casing to isolate it from outside interference. Larger bandwidth, lower crosstalk, lower line loss, and better immunity to electromagnetic interference make coaxial cable a much better medium than twisted pair for faster signal speeds. Based on the modulation technique and physical network structure, coaxial cables are generally classified in two categories: baseband and broadband.

a. Baseband

Baseband coaxial cable uses a solid center conductor with a woven mesh of copper as the outer conductor and is normally rated in the 50 ohm grades. This is the

type cable used for home cable TV or that used to connect terminal devices to time-shared host computers. Digital transmission techniques are used for unidirectional, single signal transmission. A passive transceiver is connected to the cable with a nondestructive tap for easy attachment and removal without permanent damage to the cable. Baseband means that the transceivers drive the digital data signal directly onto the cable without modulation. Various coding techniques are used but only one serial bit stream can occupy the cable at one time. Data rates in the 10-12 Mbps range are possible because the single bit stream occupies the entire cable bandwidth. This high data rate combined with time division multiplexing (TDM) techniques does allow multiple users to simultaneously access the medium with fairly high data rates and minimal delay (more detail on access techniques is presented later). Although better than twisted pair, information transmitted in baseband digital form is highly susceptible to noise and requires the use of repeaters for signal regeneration. This, together with acceptable delays, traffic load, and network configuration, normally limits the distance between stations and repeaters to one to three kilometers [Ref. 6: p. 45]. Some topologies accommodate this problem better than others.

b. Broadband

Broadband coaxial cable is the same construction as baseband cable but a little heavier and stiffer making it slightly more difficult and expensive to install. It is the 75 ohm grade cable commonly used in the Community Antenna Television (CATV) industry. Because of this common use, broadband systems can take advantage of existing CATV cabling for transmission medium plus low cost signal splitters, taps and repeaters are commercially available in large numbers. Broadband cable can handle either analog or digital signals.

Frequency and phase modulation techniques are used to transmit analog signals unidirectionally on the cable. For full duplex operation, one of two techniques called midsplit and nontranslate are used. With midsplit, the cable's bandwidth, normally 300-400 Mhz, is split in half. Signals are transmitted on one half, received at a central retransmission facility, then converted, amplified, and retransmitted on the other half of the bandwidth for receipt by all stations. Channel assignments are made by frequency division multiplexing. This allows the assignment of the entire capacity to one channel or the bandwidth can be broken into several subchannels. In the non-translate process, two cable are used; the signal is transmitted in one direction on the first cable and received in the other direction on the second. The cables are connected to a head-end device which inverts the transmission direction. Because there is a separate cable for each direction, the total bandwidth of the cable can be used rather than half the bandwidth as in midsplit. Using the entire bandwidth for one channel would result in speeds far greater than necessary for current and envisioned future network requirements. Therefore, allocation to multiple subchannels not only makes more efficient use of the available bandwidth but also dramatically increases the number of potential systems/users that can simultaneously use the same cable. The high frequency analog transmission techniques reduce the potential for interference suffered by digital baseband techniques thereby increasing the distance possible between nodes. Typical broadband networks can cover distances of 10-50 kilometers [Ref. 6: p. 45].

3. Fiber Optics

With fiber optics, the electrical digital or audio analog signal is converted to a beam of light in the infrared frequency range. This light signal is then

transmitted through an optical fiber which consists of a central glass or plastic core with a high refractive index surrounded by a cladding with a slightly lower refractive index. The difference between the core and cladding acts like a mirror for the light ray. The light transmission is based on the total internal reflection of light as it travels along the core of the fiber. The signal is transmitted from one end of the cable to the other regardless of how the cable is curved or bent [Ref. 6: p. 47].

Semiconductor lasers and light-emitting diodes (LED) are the two main light generating sources used in this technology. The lasers are more efficient because they have a narrower beam and spectral width plus they have faster optical rise and fall times in response to the input signal. However, the laser has a shorter operating life due to higher sensitivity to temperature and age.

Broader bandwidth, lower transmission losses, smaller physical size, lighter weight, better immunity to electromagnetic interference, greater electrical insulation and better security are all advantages that fiber optics enjoy over the media previously discussed. These advantages make it a prime candidate for use with LANs but this use has been restricted by high costs for system components and technological immaturity. Slow development of this technology is a direct result of poor industry standards. Different manufacturers producing various shapes, sizes, grades of materials, and connectors all act as a major obstacles in speeding development of high-performance fiber optics. The connectors in particular have been a major stumbling block. Basic limitations like maximum number of tapings, connection attenuation and reflection, plus vulnerability and link failures have limited fiber optics use [Ref. 7: p. III-62]. Its properties make it very useful in long haul point-to-point configurations such as between

LANs or nodes separated by long distances. Future continued development of this technology promises the potential for increased nodes per network, faster transmission speed, full bandwidth utilization and lower costs for node hardware.

4. Other Media

Microwave and infrared frequencies transmitted through the atmosphere have also been considered as potential transmission media for LANs. Their large bandwidths make them particularly suitable for high speed transmission. However, the added cost of expensive radio or light transmission equipment, line of sight transmission requirements, plus authorization and license for frequency usage make them less practical. Table I [Ref. 7: p. 58] offers a good comparison of the media discussed.

C. TOPOLOGIES

Another important feature of LANs is topology (sometimes called architecture) or the way in which network stations are interconnected. It is best defined as the layout of communications links, switching elements, and nodes which determine or define the path used to exchange data between any two stations. Since by definition a LAN interconnects devices in a small area, why not establish a direct point-to-point link between all stations that need to communicate? This is the philosophy behind a mesh topology (Figure 2.1). If all stations desire to talk to all others, the disadvantages of this concept are obvious. The cost in terms of cable installation and input/output hardware make it easy to discard mesh topology as a feasible approach just as the telephone industry did for wide area telephone networks. The four commonly used LAN topologies are star, ring, bus, and tree.

1. Star

Figure 2.2 is an example of how star networks connect all nodes in the network with a point-to-point link

TABLE I
LAN MEDIA COMPARISON

MEDIUM	TYPICAL AGGREGATE DATA RATE PER CHANNEL	NOISE IMMUNITY	CONNECTION	CURRENT APPLICATIONS
Twisted Pair	1 Mbps	Poor	Point-to-Point Broadcast (In Short Range)	Microcomputer Cluster PABX,CBX
Baseband Coaxial Cable	10 Mbps	Moderate	Point-to-Point, Broadcast	Office Automation
Broadband Coaxial Cable	10 Mbps	Moderate	Point-to-Point, Broadcast	Office Automation, Computer Center
Fiber Optics	50 Mbps	Good	Point-to-Point	Trunks (High Reliability Data Links)
Microwave	Up to 30 Mbps	Moderate	Point-to-Point, Broadcast	Data Link Between Nearby Buildings or Cities
Infrared	Up to 1 Mbps	Moderate	Point-to-Point	Data Link Between Nearby Buildings

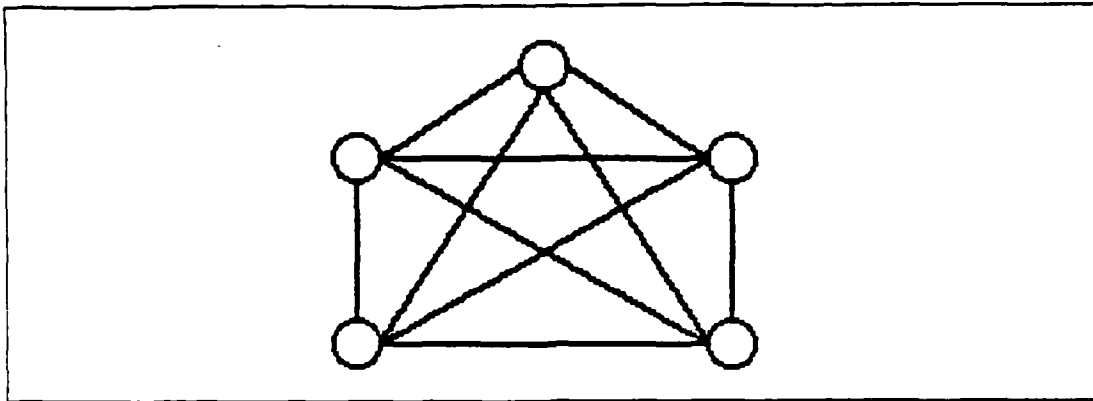


Figure 2.1 Mesh Topology.

to a common central switching or processing node. This structure is prevalent in wide area networks where centralized control is important. All communications are set up and maintained by the central node through which all traffic must pass. This is a natural extension of the time-shared host computer configurations. A good example is MCDN where front end communications processors act as a message switch for the 3270 bi-synchronous terminals attached with twisted pair.

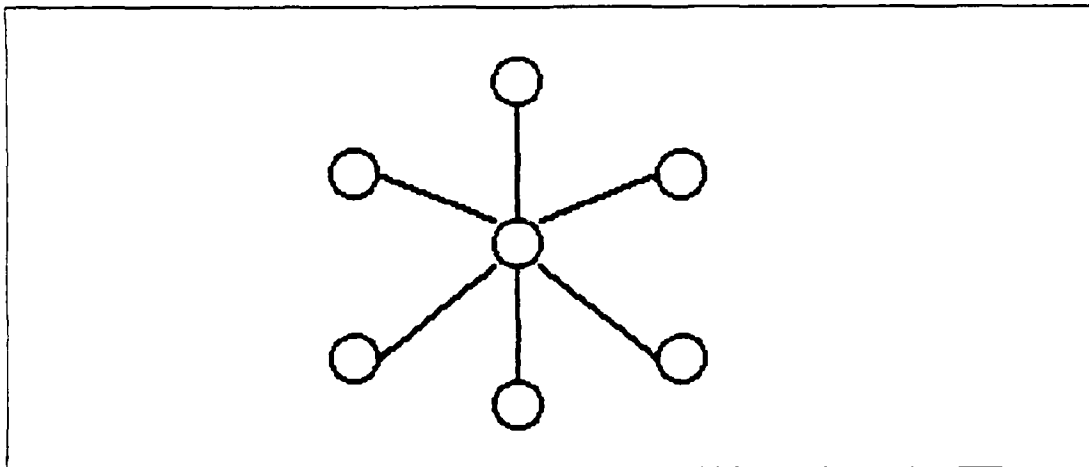


Figure 2.2 Star Topology.

Simple control structure, easy regulation of network access, and similarity (thus familiarity) to the time-shared systems are all advantages of the star network. Central processing places minimal burden on the stations but by the same token makes the central node more complex. A significant advantage of the star topology is that it can utilize the existing star-based telephone network cabling already installed. This cabling together with a PBX or CBX that can handle data switching offers a relatively inexpensive local area network. Many integrated and dedicated data PBX's can make immediate use of the installed wire resources saving considerable cost on cable installation. If the switch in use cannot handle data, a significant investment is required to buy and install one that does. The greatest disadvantage is total reliance on the single central node which, when it fails, brings down the entire network. The network is also limited in expandability to the maximum number of stations the central node can handle. Large volumes of traffic may cause serious delays at the central control point.

2. Ring

A ring or loop network (Figure 2.3) is a set of nodes in a closed loop of cable with repeaters connected on either side with point-to-point circuits to two other repeaters. Messages are placed on the ring in one direction using time-division multiplexing that either assigns the time slots permanently (slotted ring) or on demand (token ring or contention ring). Control of the time-slots, which in turn controls access to the network, can be centralized in one node or distributed among all the nodes. More information on access methods is provided in the next section. The ring structure is often called active because as messages move around the network, all nodes or repeaters actively participate. Each one accepts its own messages and passes on messages destined for others. The biggest

advantages of the ring are ease of message routing, low cost, and relatively easy expandability. On the negative side, a single break in the ring can bring down the entire network. Some vendors have defeated this problem by using by-pass relays to eliminate the path through failed repeaters or dual cables to by-pass failed cable sections. As the ring gets larger, the round trip delay for the message can be a significant problem in some control structures. Adding new nodes to the ring is limited only by the maximum addressing capability and the maximum allowable physical distance between repeaters.

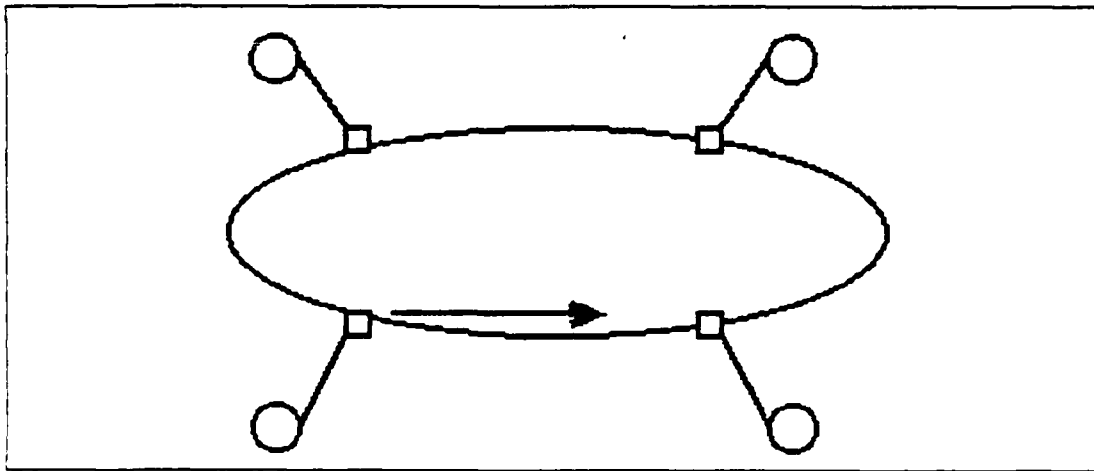


Figure 2.3 Ring Topology.

3. Bus/Tree

A bus is simply an unclosed two way ring/loop network that does not use active repeaters (Figure 2.4). Each station has a single unique address for identification during transmission and receipt of messages. The simple passive interface gives the bus the advantages of the ring/loop topology without the disadvantage of one failure bringing down the network. All stations connect to the main transmission line or bus and the transmission from any station propagates the length of the bus received by all

stations. Bus topologies are more complex in terms of the contention control schemes needed to determine who transmits when. Control can be centralized or decentralized. When centralized, a network controller is used to poll all nodes or receive transmission requests then grant access authority to individual nodes. When decentralized, a contention scheme is used by all stations to control network access. The number of allowable nodes is once again limited by the addressing scheme and propagation delays associated with the length of the bus. Performance is determined by the bandwidth of the bus, number of nodes, access method, and traffic load.

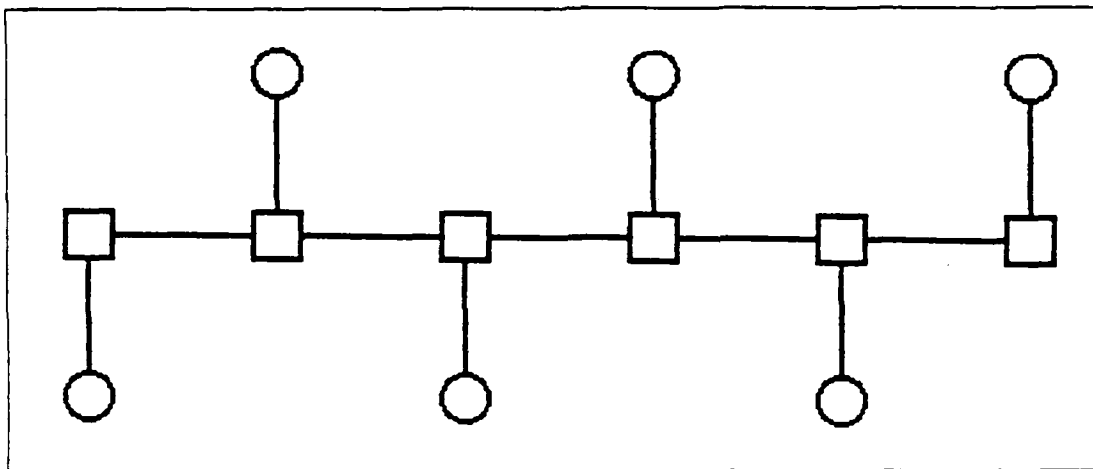


Figure 2.4 Bus Topology.

The tree topology is a form of bus topology where the medium is a branching cable with no closed loops (Figure 2.5). Transmission from any station propagates throughout the medium and is received by all others. Bus and tree topologies are often called multi-point or broadcast [Ref. 8: p. 56].

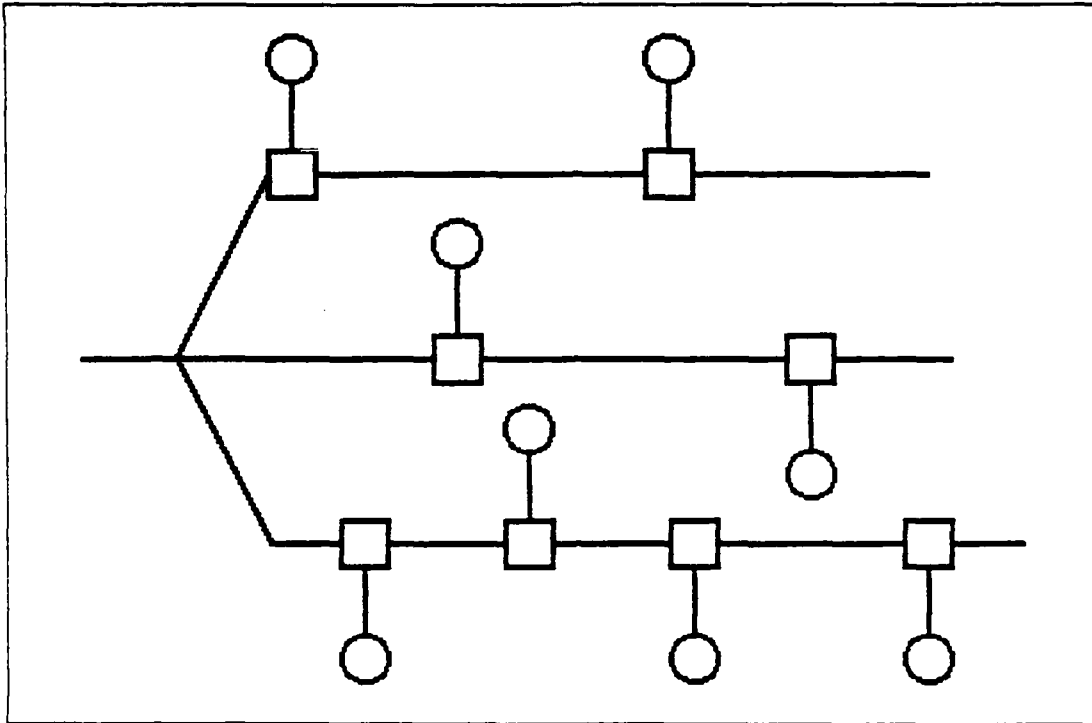


Figure 2.5 Tree Topology.

D. ACCESS METHODS

Use of a shared local network requires that any station wanting to transmit must first gain access to the network. Different access methods offer different characteristics. Therefore, traffic volumes plus time sensitivity and sequencing of the data are characterized to determine which method is best suited for the network to be installed. Once a station gains access to the medium, it can either exhaustively transmit all frames awaiting transmission or transmit only a maximum number of frames per attempt. Access methods can be centralized, where a central arbiter has control over access by the other nodes, or distributed. Distributed control allows individual user devices or network interface devices to control their own access. Time division multiple access, circuit switching, and reservation are examples of centralized access while token passing and Carrier Sense Multiple Access (CSMA) are distributed examples.

1. Time Division Multiple Access (TDMA)

This method permits all devices to share the transmission time one at a time. This is done in a predetermined sequence or based on need to transmit determined by polling queries from the central arbiter. The main idea is to allocate access to the medium in a deterministic, equitable manner. MCDN is a good example of this method where the front end processor polls line devices for traffic. Another variation of this method is called slotted TDMA. The available time is broken into time slots of equal length which are allocated to the various devices on the network. Devices only send in their assigned slot and only for the duration of that slot. If the message does not fill the slot, the unused portion goes empty. If it is longer than one slot, it is broken up and sent over several slots. All stations must be able to detect the beginning and end of each slot so synchronization is critical.

The last variation is called slotted ring which also involves a fixed number of slots of equal duration. All slots are initially marked empty using a status bit at the beginning of the frame. If a station wants to transmit, it waits for an empty frame, changes the status bit from empty to full, and inserts a frame of data as the empty slot goes by. Normally, the frame also contains two response bits which are changed by the receiving station to indicate accepted, busy, or rejected. The slot returns to the source and is marked empty or refilled based on the response bits. Other variations may allow change of the status bit by the receiving station based on successful receipt of the frame.

2. Carrier Sense Multiple Access (CSMA)

CSMA is used in networks with common transmission media like the bus and tree topologies. Each node contends for access or control in a decentralized manner. In this method all devices must be able to listen to the network and

detect if other devices are transmitting. If a transmission is in progress, then the listening device will wait until the line is clear before transmitting. A second feature can be added to this method called CSMA collision detection (CSMA/CD). During heavy traffic periods, several devices can be waiting to transmit, which could cause a collision if all begin at the same time. Collision detection allows a sending station to listen while transmitting and if it detects the presence of another signal besides its own, it will stop transmitting and back off for a random amount of time before trying again. Some systems also have the transmitting station that detects the collision send a jam signal to ensure none of the receiving stations try to interpret the bad data. This also allows buffers holding any of this bad data to be cleared. The random back off reduces the statistical probability of a second collision with the same station. As more devices attempt to transmit in a network using CSMA/CD, network efficiency declines because of the increased time spent resolving collisions. Mixing devices that send long messages with those that send intermittently also increases the probability of collision. The random versus deterministic properties of this method offer excellent performance at low load levels. However, applications which require known transmission delays and guaranteed access, such as digitized voice or synchronous devices, find this method unacceptable.

3. Token Passing

In token passing systems, a unique sequence of bits depicting a free token is circulated from one node to another in a predetermined sequence. If a node has data to transmit, it changes the token bit sequence to indicate busy then sends its traffic. After transmission, the sending node changes the token bit sequence back to free and sends it on to the next node in the access sequence. The only

network overhead is the token bit sequence which is a fixed length so maximum delay can be calculated. Other advantages include high transmission efficiency for varied packet sizes and data rates, reliable operation under all load conditions, and freedom from collision detection requirements. Token loss or damage and fixed response time, even during light load conditions, are the two biggest disadvantages. Token loss or damage is usually solved by using a network monitor which keeps track of the token's status. The monitor may also take on the responsibility for reconfiguration of the token passing sequence as stations enter and leave the network.

E. PROTOCOLS AND STANDARDS

1. General

Exchange of information among information systems is a complicated process. The required cooperation must be formalized in rules which define the methods, procedures, and conventions needed to complete the information exchange. These rules, called protocols, are the common tools designed to control information transfer between computer systems. They are imbedded in specific elements of the information system and are designed to effect the movement of information, ensure mutual understanding, and to provide error control and recovery procedures.

Early experimental computer networks were developed independently which resulted in the creation of many different architectures and conventions for interconnecting equipment. These differing approaches were often proprietary and generally incompatible. The growth of automated information processing, the requirement for distributed elements to interoperate, and the cost inefficiency of dealing with incompatible protocol architectures highlighted the need for standardization.

2. The OSI Model

In 1977, this need for standardization was recognized by the International Organization for Standardization (ISO) and a special subcommittee was created to develop a standard architecture for Open Systems Interconnection (OSI) [Ref. 9: p. 425]. The subcommittee's objective was to develop a standard international standard open system architecture which, if followed, would enable heterogeneous system interconnection and communication. Early discussions resulted in the agreement among subcommittee members to develop a layered architecture which would break the complexities of data communications into manageable portions. A logical structured sequence of layers would be specified, each of which would handle specific functions. They would be designed independently however, each would support and interconnect with the layer above and below it. Each layer would, through the layers below it, interact with the corresponding (peer) layer located in the other information system elements. The subcommittee's first 1.5 years of work resulted in the layered ISO OSI reference model (OSI/RM) (Figure 2.6). The outside boxes represent the common layers at each data terminal equipment (DTE) location. The center three boxes represent the layers employed by data circuit-terminating equipment (DCE) when an intermediate network is used for long distance transmission between more than one DTE local network. This layering approach offered the following advantages taken from [Ref. 4: p. 5-76]:

- Any given layer can be modified or upgraded without affecting the other layers.
- Modularization by means of layering simplifies the overall design.
- Different layers can be assigned to different standards committees or different design teams.
- Fundamentally different mechanisms may be substituted without affecting more than one layer (e.g., packet switching versus leased-line concentrators).
- Different machines may plug in at different levels.

- The relationships between the different control functions can be better understood when they are split into layers. This is especially true with the control actions which occur sequentially in time from layer to layer.
- Common lower level services may be shared by different higher level users.
- Functions, especially at lower layers, may be removed from software and built into hardware or microcode.

There are some disadvantages. However, when compared to the advantages, their impact is slight.

- The total overhead is somewhat higher.
- The communicating machines may have to use certain functions which they could do without.
- To make each layer usable by itself there is some small duplication of function between the layers.
- As technology changes (e.g., as cryptography and compaction chips become available, or these functions can be built onto chips) the functions may not be in the most cost-effective layer.

A number of principles were used by the ISO subcommittee to arrive at the seven layer OSI/RM. Things like minimizing the number of layers, creating boundaries to minimize the number of interactions across them, collecting similar functions in the same layer and some 10 other principles were considered to arrive at the specified functions in each layer [Ref. 9: p. 429]. The layers are often broken into two basic levels: low-level protocols (levels 1 & 2 in the OSI/RM) and high-level protocols (levels 3-7). The low-level protocols identify the basic conventions used to transport the data signals (bits) through the network in a timely and reliable manner. There is no real concern for the meaning of the bits being transmitted. The high-level protocols, on the other hand, transmit and interpret the meaning of the bits and data structures used to communicate and support end user applications. In a sense, the low-level protocols provide a foundation to support the high-level protocols which in turn support the user. Each layer or level uses functions provided through the level below them and provide new or additional functions to the levels above.

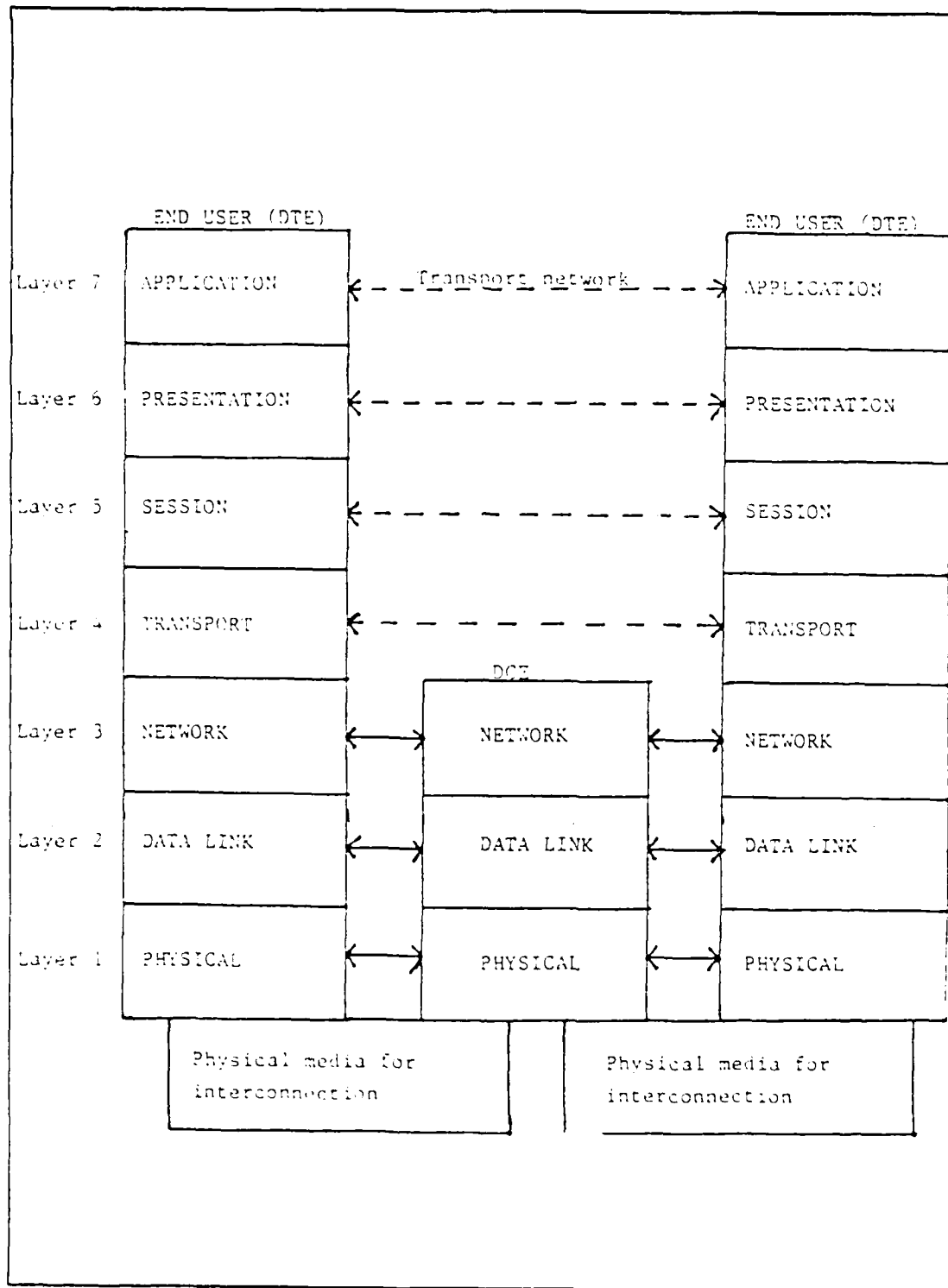


Figure 2.6 ISO Open System Interconnection Reference Model (OSI/RM).

a. Physical Layer

The physical layer is concerned with the transmission of raw data over the transmission medium. It provides the electrical, mechanical, functional, and procedural characteristics like voltages, connectors, frequencies, modulation, etc, used to establish, maintain, and release physically connected data circuits between DTEs.

b. Data Link Layer

This layer contains the control functions or rules needed to reliably transfer data over the communications link established by level 1. The data link rules define initialization and synchronization; control errorless data interchange with addressing, frame sequencing, request and acknowledge, error checking, etc; terminates data transactions; and provides for recovery from abnormal conditions like invalid or lost responses, loss of synchronization, and faults caused by noise, interference, or failure of the physical link. [Ref. 10: p. 445]. These protocols were originally character oriented to support the early synchronous bulk data transfer requirements. However, because of the high overhead involved for short bursty transmissions, which characterize the newer interactive applications, bit-oriented protocols were developed. This shortened and streamlined data link procedures.

c. Network Layer

The network layer manages the routing of messages from sender to destination and, when more than one path is involved, selects the route that best suits network conditions to prevent congestion. This layer relieves the transport layer of responsibilities for routing and switching. Because of their broadcast nature, network services are not required when dealing with local area networks. However, layer 3 is vital to successful communication between LANs or between a LAN and a WAN.

d. Transport Layer

The transport layer is the end-to-end layer that provides a transparent means of transferring data for the session layer above it. It segments the message into manageable parts or packets sized to fit the network being used for transmission. At the destination, these packets are reassembled and sent to the destination session layer.

e. Session Layer

This layer is the user's interface to a network. It involves a set of log on and dialog rules that enable the user to logically interconnect with various remote hardware/software locations. It essentially controls, delimits, and synchronizes the data operations between two presentation layers.

f. Presentation Layer

This layer involves the management of the exchange, display, and control of the structured data from the applications layer. The applications layer selects the set of services like data content architecture, data interface architecture, data compression technique, encryption, etc, which enable it to interpret or encode the data being exchanged. It ensures that the information exchanged between application layers is meaningful.

g. Application Layer

This is the highest layer in the OSI/RM architecture. It directly serves the end users through the use and interpretation of content (meaning), semantics, and syntax involved in normal person-to-person communications. It involves the function needed to initiate, maintain, terminate, and record data transfer between two applications layers.

3. LAN Standards

Along with the ISO subcommittee's OSI/RM came a recommendation to begin projects to develop protocols for

specific communications networks including LANs. LAN facilities and standards tend to cover only the physical and data link layers as depicted in Figure 2.7 from [Ref. 11: p. 191]. However, some vendor software and hardware combinations may involve all seven layers to permit interaction like personal computers communicating with a host computer at the applications level. When a single vendor provides this kind of complete network services, he tends to work out interfaces and protocols to get the best performance from his own product. If a system is pieced together in this manner, complete understanding of the vendor's interfaces and protocols is imperative.

In the absence of accepted standards, vendors tend to develop their own. They hope that industry and individual buyers will rally around these "defacto" standards to encourage their acceptance at least nationally. This is exactly the case with LAN standards. In February 1980, shortly after the ISO subcommittee recommendations were submitted, Project Group 802 of the IEEE Computer Society was set up to develop LAN standards. Three working groups were established, two to define standards for the physical and link layer protocols with a third to act as liaison with higher network layer projects. This third group was also chartered to provide guidelines for the standards to satisfy user needs with respect to existing higher levels, inter-network, and network management issues.

DEC, Intel, and Xerox immediately submitted detailed specifications for a well-known CSMA/CD, bus, coaxial cable system known as ETHERNET. They proposed that ETHERNET be accepted as "the" LAN standard. However, early IEEE sessions surfaced strong opposition from advocates of token passing, particularly Honeywell and IBM. Later that year the conflict was resolved by breaking working group 1 into subgroups which were directed to develop CSMA/CD and token

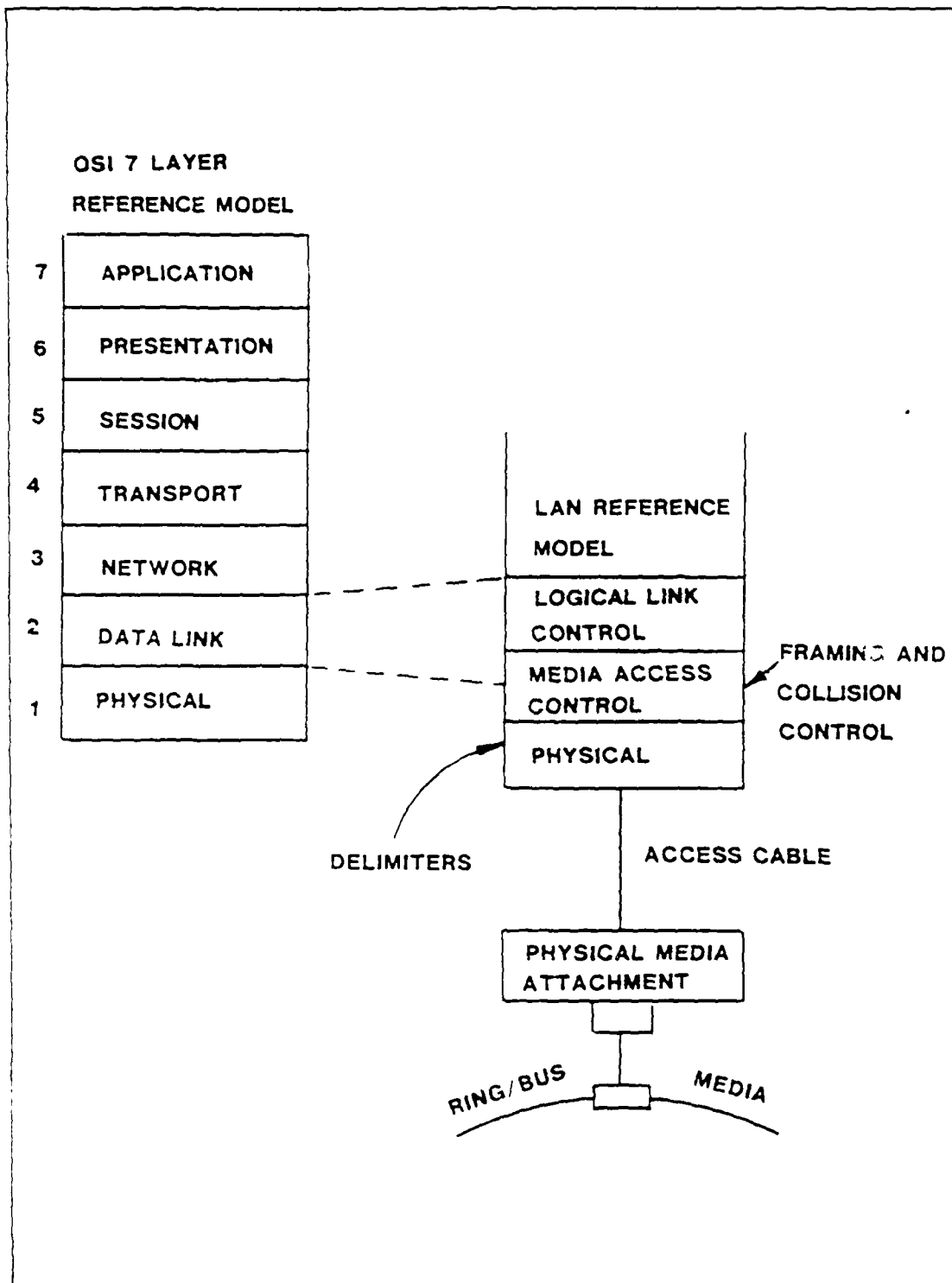


Figure 2.7 Relationship Between OSI/RM and LAN Standards.

passing methods in parallel. A demand was also made to make all specifications identical except for the algorithm itself (i.e. addressing, frame format, coding method, etc,). The subsequent proposed changes to ETHERNET from those supporting token passing brought progress to near stand-still. Finally, the ISO decided to not only include CSMA/CD and token passing as separate bus broadcast standards but also to develop token passing in a sequential topology, the token ring. The current IEEE 802 committees have the following responsibilities [Ref. 12: p. 358]:

- 802.1 Higher layer protocol liaison
- 802.2 Common logical link protocol
- 802.3 ETHERNET or CSMA/CD bus access method
- 802.4 Token passing bus access method
- 802.5 Token passing ring access method
- 802.6 Metropolitan area networks

According to Roelandts [Ref. 13: p. 231], 802.3 and 802.4 standards have completed the approval process and are now recognized standards. 802.5 is still in process and manufacturers are having difficulty implementing this complex standard in silicon. The availability of network controllers integrated on a chip brings down the price and raises the volume. This is the normal ticket to success for a protocol. However, the fact that IBM (controller of 65% of the computer market) supports 802.5 may be the ace in the hole it needs to survive.

4. High Layer Protocol Standards

The physical and link layer protocols are very important when desiring compatibility on a single LAN. This is where most LAN standards activity has been concentrated. However, standards at the network layer and above are critical for compatibility and communication LAN to LAN or LAN to WAN. These are the protocols that affect the user's ability to do things like access a remote computing resource

and other users, transfer files from one system to another, or send mail to other users on the network.

Before LANs, long distance network protocols were oriented toward data communications rather than networking. These protocols supported the communications required by terminals connected to a host computer which in turn was connected to one or more other hosts with their own terminals. The emergence of LANs generated a new need for tying together networks that already had their own network access and message transmission and reception protocols. Initially, design concentrated on the terminals in these networks. However, that emphasis has now shifted to providing long-distance access to self-contained local networks that have their own protocols for communication among the local workstations. This concept caused designers to view the local area network as a single terminal [Ref. 5: p. 15-16].

About the same time that LAN protocols were beginning their design and specification phase, long distance public data networks were growing rapidly and their protocols were relatively mature. The International Telegraph and Telephone Consultive Committee (CCITT) had already established recommended standard protocols for both synchronous circuit switched and asynchronous packet switched data networks. CCITT X.21 is the general purpose interface between data DTE and DCE elements for synchronous operation on public data networks. CCITT X.25 is the standard device-independent interface between packet networks and user devices operating in the packet mode. These protocols concentrate on the first three layers of the OSI/RM for DTE/DCE connection (Figure 2.6). Both are primarily network layer protocols consistent with the OSI model for distribution of functionality among layers. DOD used the OSI model and packet switching features of X.25 to come up with its

own network model. This model not only supports the open system model concept but also incorporates special features to enhance reliability and to support special DOD security requirements.

DOD began experimenting with the X.25 packet switching protocols during the development and implementation of the ARPANET protocol suite. This work resulted in the DOD INTERNET model (not formally defined until 1982) which has guided the implementation of many DOD protocols and communications networks since the early 70's. This model emphasizes internetworking of computer systems through communications subnets for host-to-host communications, subnet-to-subnet communications, and resource sharing. The idea is that each subnet has its own set of protocols which may or may not be the same. They communicate with each other through gateways to the WAN. This is achieved through two companion protocols called Internet Protocol (IP) and Transmission Control Protocol (TCP) [Ref. 7: p. III-46]. IP provides datagram service for applications sensitive to fast, nonsequenced delivery across several networks. TCP uses the services of IP plus sequenced delivery, flow control, and end-to-end acknowledgement to offer a virtual circuit service for applications that require interactive terminal to remote host processing. Figure 2.8 shows how the DOD INTERNET Model matches up against the OSI/RM. Problems with adoption of the OSI transport layer protocols have been difficult to resolve because of the existence of both the connection-oriented virtual circuit and the connectionless datagram service. As a result, five different classes of service, which provide varying degrees of reliability, have been established for the OSI transport layer. This multi-class approach will have significant negative effects on reliability of internetworking communications. It will cause increased opportunity for undetected errors or

lost messages due to their different characteristics. The Defense Data Network (DDN) TCP/IP falls in the class 4 category which is the most complex. Proponents of TCP/IP are currently trying to convince the major standards organizations to adopt them as "the" networking protocol standards for long distance networks. They are already mandatory in all DOD packet switching networks which connect or have the potential for utilizing connectivity across network or subnetwork boundaries [Ref. 7: pp. III-46-III-48].

There is a great deal of discussion among DOD network designers regarding whether to require TCP/IP in LAN protocol design. Proponents argue that this would greatly enhance reliability and speed transmission through gateways at the LAN/WAN boundary. They say it would reduce the costly complex functions of higher layer protocol translation and mapping. An additional benefit would be increased speed through the gateway due to the decreased protocol translation. Opponents argue that the LAN overhead costs associated with such a move are unnecessary for subnets whose communications and information exchange are primarily local. Only significant testing and modelling will determine whose argument is correct.

F. PBX TECHNOLOGY

The logical and insistent move from analog to digital transmission techniques has precipitated an evolutionary change in telephone switching equipment. Early first generation step-by-step mechanical private branch exchange (PBX) telephone switches were replaced by second generation electromechanical common control devices. This happened when the telephone industry borrowed stored-program control from the computer industry. Recognizing the growing need to switch data as well as voice, third generation PBX's were developed to digitize voice signals either at the telephone instrument or through a line card at the PBX. Voice and

OSI	DOD
Application	Application
Presentation	Presentation
Session	Session
Transport	Transport (TCP)
Network	INTERNET (IP)
LINK	
	LINK
PHYSICAL	PHYSICAL

Figure 2.8 OSI/DOD INTERNET Comparison.

data terminals can now access the switching equipment on the same line. This not only enables voice and data to use the same medium and transmission equipment but also facilitates transmission between switching nodes by multiplexing both signals with TDM techniques. Since the system uses the same twisted-wire telephone cable for voice, data, and control signals, it is a cost effective way to satisfy both voice and data switching requirements. It is important to recognize that the third generation switch technology reflects the prevailing concern of the middle and late 70's which was digitized voice. They treat data as an add-on capability which is normal because voice telephone calls are still the main source of business. This step child treatment results in relatively slow transmission rates: 19.2 kbps for asynchronous RS-232C data interfaces and up to 64 kbps for synchronous data interfaces. A limited protocol conversion capability for asynchronous data packetizing functions is provided on some vendor offerings. These rates may satisfy the needs of many office automation requirements but come nowhere close to LAN speeds offered for mainframe access, file transfer, program sharing, and micro-to-micro communication. These switches were not designed for high-speed packet switching. Many data switching network buyers are looking for a better solution than using existing PBX assets for voice and low speed data transmission and then adding a second parallel network to handle high speed data communications. The maintenance and expansion of multiple networks can prove to be costly and highly inefficient. The recent fourth-generation PBX products take the digital switching technology a step beyond voice/data integration into a world of enhanced networking capabilities.

Fourth-generation PBX (often called CBX) systems combine advanced voice communication features, high speed data transmissions, and integrated LAN capabilities. Such

systems could potentially meet all needs in one integrated network which would allow sharing of valuable resources as well as consolidation of network management facilities. According to Jewett [Ref. 14: p. 47a], the following five major capabilities differentiate a fourth generation PBX from the third generation.

- The fourth-generation PBX includes an integrated LAN that is intrinsically part of the PBX architecture, thus providing the potential for fully integrated wide-band data transmission as well as voice and message communications.
- The dynamic allocation of bandwidth depending on the size and nature of each transmission. This is the principal technology advance that sets it apart from third generation. Dynamic bandwidth allocation allows the system to grow as user requirements grow which should enable accommodation of many future wideband demands.
- The ability to integrate a packet channel to each terminal in the system - a packet channel that is accessible by the user's data terminal equipment. This allows the system to handle data in an efficient manner, in packetized form, from originator all the way to a local computer/file server or through a WAN to other host computers.
- Offers a layered software structure (like a minicomputer) that provides for the integration of message communications at every level. Technically, this allows the linking of text messaging with active call processing which allows the use of mail boxes and automatic call return with the touch of a single button. The system offers an easy to use message telephone that tells the user what to do with the touch of one button.
- The system is fully distributed. The PBX nodes can be spread over wide geographic boundaries while continuing to provide fully transparent communication with other nodes on the system. In addition, each node can function as a stand-alone PBX. The network manager has the choice of distributing nodes throughout the area to be serviced or placing all nodes in one room like traditional PBX facilities.

Although these new fourth-generation switches offer many new technological advantages, traditional star topology disadvantages like central point of failure, central node complexity and along with it high cost, etc, still exist. Characterization of current and future user needs as well as inter-networking requirements and standardization will likely determine whether this is a viable networking alternative.

III. A STRATEGY FOR LAN SPECIFICATION

A. GENERAL

Today's environment for the LAN system designer is much like that depicted in Figure 3.1: Where does one begin? The early 80's approach to solving this problem is a bottom-up design. With this approach the customer buys workstations assuming that a system exists that will eventually allow him to connect these workstations together and do something meaningful. A common myth that fuels this approach is that communications networks like LANs can interface with a variety of other heterogeneous networking techniques such as X.25, SNA, etc, using asynchronous, synchronous, serial, and parallel interfaces. Another myth is that buying a network is as easy as calling a networking specialist, having him install his product, then just plug in the the workstations and the system works. These two myths along with the confusing vendor claims of universal interconnection and communications solutions have driven users to choose and install what appears to be the latest technology. They choose the system with the highest bandwidth, the largest number of devices, and multiple information types. In other words, the network was specified and chosen based solely on the technical specification of one networking solution--the LAN. Because the network was essentially specified by the vendor's description of what it could do vice the user's detailed description of what was needed, these networks have few problems passing operational acceptance criteria. It is only after network installation and acceptance that the organizations discover that there were other issues which should have been resolved prior to or during the LAN specification/selection process.

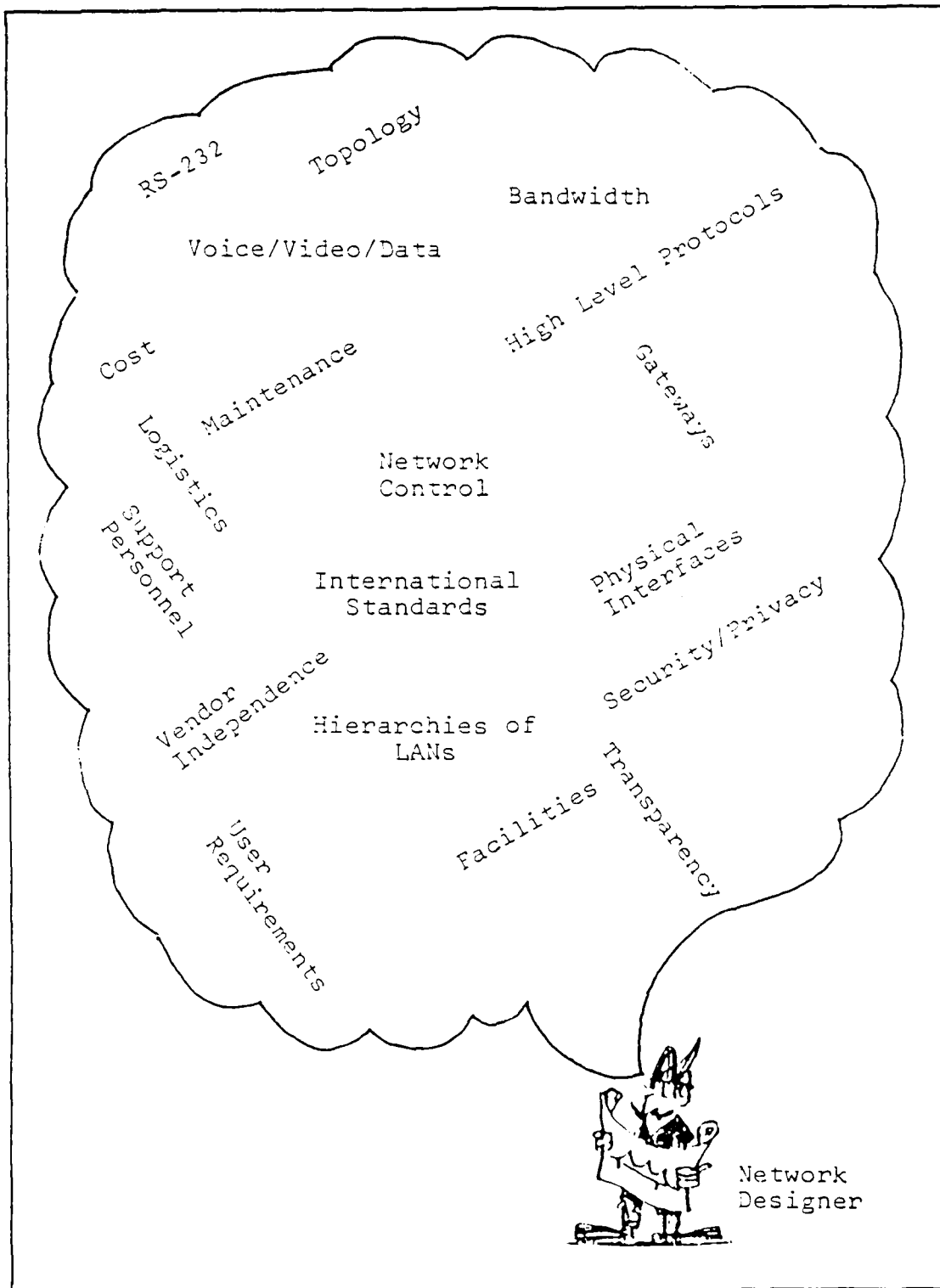


Figure 3.1 LAN Specification: Where to Begin?.

LANs suffer the same fate as numerous previous network designs. The subnetwork (LAN) is designed first by network specialists based on low-level technical and logical performance criteria with high-level services and functions designed later, again by network specialists. The end user's needs are a low priority in this process. It usually takes years of coordination between user and designer to "modify" the original design to arrive at acceptable high level services and protocols to support them.

A more appropriate strategy is one that adopts a system versus component approach looking at things from the top down rather than the bottom up. A close partnership between users and information system professionals is essential. You need to characterize the applications or end user requirements to be supported, the interconnection and communications services required by user applications, and the technology available to support these requirements in that order. This should be done first from a functional, not necessarily technical standpoint. Obviously technical terms are often necessary to describe the application, but the emphasis here is on the need not the solution. Mistakenly, people often say they have a requirement for a LAN. A LAN is not a requirement but rather an element in a list of potential solutions for satisfying an information processing and transfer requirement. Once the user's need has been properly characterized, a layered system design approach concentrating on connections between layers to optimize performance and functionality can begin. Figure 3.2 depicts the sequence that will be used in this chapter for specifying and in the next chapter for selecting a LAN.

B. USER REQUIREMENTS

The first step in this process is characterization of the users which leads to characterization of their information transfer needs. An identification of the

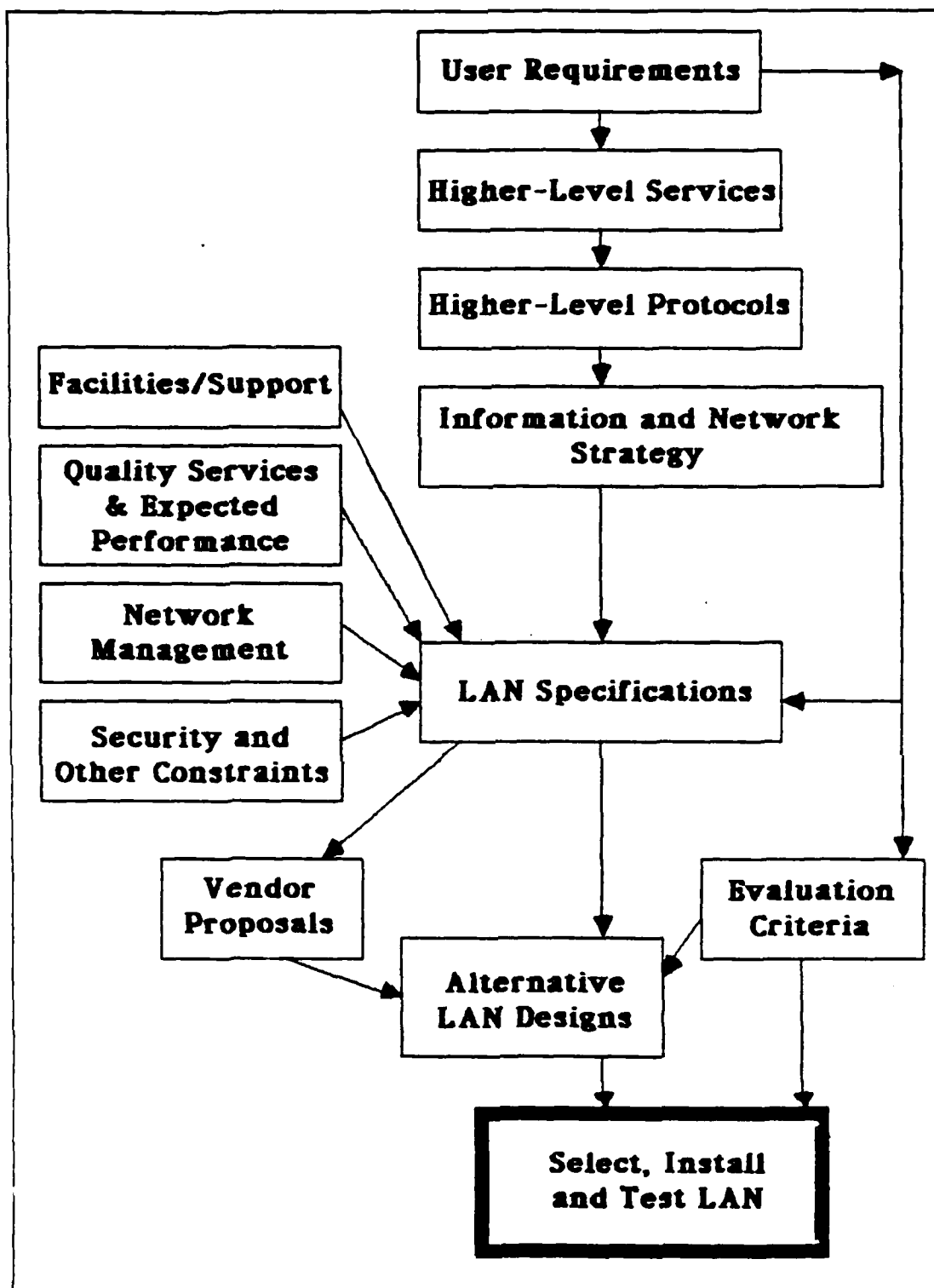


Figure 3.2 LAN Specification/Selection Strategy.

mission and functional responsibilities to accomplish this mission is the best point of departure. Taking these functional responsibilities to the lowest level of detail will permit subsequent translation into protocol groupings (application, presentation, session, transport layers). This grouping will identify unique protocol requirements as well as common services shared by many functional requirements. Labor and paper intensive procedures should be eliminated or reduced by automated tools where affordable productivity gains can be achieved.

Once a concise complete list of functional responsibilities is compiled, the current organizational and operational management structure can be drawn depicting how these mission functions are handled. Adding the information sources and current data flow techniques used to connect information sources and functions in the existing management structure will facilitate identification of information transfer deficiencies as well as connectivity and capabilities that already exist. While the objective is to eliminate obsolete end-user technology, a certain degree of current system upgrade or perhaps total accommodation of existing equipment/network procedures and interfaces will be appropriate. Known ongoing system upgrades and improvements (i.e. new telephone switches, cable plant improvements, recently acquired intelligent workstations, etc,) should be addressed when identifying deficiencies. Separate explicit and comprehensive individual deficiency descriptions in terms of functional requirements will allow accurate evaluation of their scope. Users must first understand their underlying information needs without regard for the specific solution that will be used to satisfy these needs. New emphasis is needed to ensure that users understand these needs well enough to completely and accurately define them for the network designer. This way the designer fully

understands the necessary information flows both vertical and horizontal. Identification of capabilities that already exist will alert the network designer and specification preparer to required (at this point) logical information interfaces that must be satisfied.

Identification of the ultimate source of the information and all handling points in between may allow the secondary benefit of eliminating those points whose only function is distribution. The degree of resource clustering to support applications along with the identification of distributed versus centralized processing are additional off-shoots of this analysis process. Individual information systems are seldom truly autonomous units because often the same information must be moved from one system to another. This creates a need for interoperability or sharing. By making this kind of comparison and developing these relationships, the individual systems become part of a broader framework of systems thus depicting an architecture of local user needs.

Several different manual as well as automated methods of requirements analysis exist for defining, developing, or improving information systems. Activity studies, review of local directives detailing required information submissions, and questionnaires can all be used in quantitative (linear programming) and qualitative studies for requirements identification and analysis. The result should be a priority list of different information subsystems broken into functional areas across command and staff channels. The next step is to design equipment independent data/voice system solutions to satisfy the specified information subsystem requirements.

Devices currently installed in most user work areas are not compatible because they evolved from programs designed to satisfy differing requirements. However, these devices are now crossing over many traditional boundaries.

Telephone systems now include features that border on data processing, data processing includes office automation which crosses into traditional administrative services, and small computers sometimes give users more powerful software tools than available in large scale data processing systems. The objective of any user requirements study should be the identification of needs in a way that permits adoption of a flexible and dynamic open-ended information handling system. This type of system integrates all the technologies of data manipulation, text processing and communications. The ultimate goal may be multi-function workstations that offer a wide range of information handling tools. These workstations could provide the user with an easily understood information system interface which is common among individual applications. Moving information between applications without labor intensive intermediate handling or reformatting in a manner that supports the way people really work and think will be the key to success in this environment.

A poorly designed and managed information system is just as big a contributor to the problems generated by isolated individual information processing as the standalone personal computers. Significant changes in operating procedures, no matter how well intended, can cause severe problems with user performance. Examples of the problems caused are: 1) A breakdown of the standard organizational information flow and processing procedures. This can easily lead to a proliferation of unique procedures for handling different kinds of data among people and groups in the organization. 2) The organization loses control of its information resources. Since information is an organization's most important resource, isolating and thus fragmenting processing and storage resources can lead to an inability to allocate them for the benefit of the whole. 3) Security and

integrity of data are lost. Intelligent workstations operating in isolation are still powerful tools for manipulating data. However, it is quite easy for individual users to change or lose data without realizing it. 4) Disruption of established work flows that support the organization's mission functions and operations. [Ref. 15: p. 258].

As individuals or individual parts of the organization become more productive, it affects everyone else whose work is connected to them. Adequate planning and preparation is essential to address changes in work responsibilities and behavior patterns, accommodate user concerns, and allow smooth transition to the new capabilities. By looking at all these factors in depth, an information system architecture supported by one or more processing and networking strategies can be developed. The solution is not known before or during the analysis so the results should not be slanted toward a particular technological solution. A final goal is to perhaps develop standards and guidelines which ensure individual projects/programs maintain overall compatibility in specification and selection as well as installation, operation, and maintenance.

The following is an example list (certainly not exhaustive) of broad functional categories that could evolve from this analysis:

- Message and document filing, retrieval, distribution, creation, and revision.
- Job entry on a host or mainframe
- Interactive terminal operations with a host or another terminal
- Resource allocation
- Program-to-program operations user-user, user-host, etc.
- Artificial intelligence/expert systems
- Computer aided design and engineering (CAD/CAE)
- Voice transmission in a distributed environment.

Each of these broad functional categories can then be broken into subfunctions which state more specifically the user's needs. For example, Table II shows the subfunctions for the message and document category. Subfunctions in this kind of detail for each major functional area ensure that no subfunctions necessary to accomplish the mission are omitted when selecting the appropriate technology. The next step is to take these functional categories and translate them into higher-level services.

C. HIGHER-LEVEL SERVICES

This is where we begin the process of identifying the specific technology best suited to satisfy all the functions and subfunctions listed in the analysis above. Data, voice, video, and imagery are all examples of information formats that can be processed and transmitted through a network. The form of the information as well as the ability to change from one form to another without reducing integrity or content should be considered equally with the information source and the destination. Can it be processed and passed in an equal priority connectionless manner or is a highly interactive dedicated connection environment the only feasible solution? This is one of many questions to be asked when translating from user requirement functions to applications. These applications must be further translated into services and protocols designed to support the requirements. Characterization in this manner will facilitate future tradeoff decisions on multiple information types versus handling characteristics (speed, time-of-service, etc,) for any one type.

Numerous software and hardware tools used to satisfy the users insatiable desire for information have led to the development of services common to many different applications. Database management, office automation, digitized voice, and higher-order languages for end-user software

TABLE II
MESSAGE AND DOCUMENT HANDLING SUBFUNCTIONS

1. Messages
 - a) Ability to transmit information messages
 - b) Ability to store, distribute messages
2. Information Filing and Retrieval
 - a) Centralized filing with multiple-user access
 - b) Multiple level storage (diskette, central unit, host)
 - c) Authorization levels (view only, view and print, print only, edit, edit and print, private (no access))
 - d) Versatile indexing
 - e) Purging capability
 - f) Sufficient capacity for storage (growth)
 - g) File maintenance (add to, delete, change)
 - h) Immediate automatic filing
3. Information Distribution
 - a) Electronic transmission of documents and messages
 - b) Ability to browse index of mail box
 - c) Automatic standard distribution lists
 - d) Acknowledgement of receipt/delivery
 - e) Access authorization for mail box use
 - f) Annotate documents, redistribute, file purge
 - g) Priority document indication
4. Information Creation and Revision
 - a) Sophisticated editing functions (spelling check, deletion, move paragraphs, reformat, etc...)
 - b) Merge capability (generation of repetitive letters, text and files, text and data)
 - c) Ability to electronically store/retain what is created
 - d) Retrieve for document creation (boilerplate, standard paragraphs, etc...)
 - e) Quality print capability (versatility in type styles, formatting)
 - f) Sufficient integration to allow for segmented creation and revision
 - g) Automatic generation of charts, graphs
 - h) Mathematical capabilities
 - i) Creation and maintenance of file information currently on lists
 - j) Simultaneous input/output

development are all examples of services supported by today's technology. These services depend on software oriented applications like file transfer, virtual terminal, terminal emulation, and job transfer and manipulation to accomplish the needed operations. The set of functions from user requirements can now be grouped and treated as an application or multiple applications. Although grouped for purposes of identifying common applications and services, the identity of individual functions and subfunctions must be preserved for future development of specifications as well as test and evaluation objectives and procedures. They will be the heart of specifications used to solicit bids from potential vendors and later as the basis for test criteria against which the installed system can be measured.

Various information systems use applications processes or logical elements to perform the services required by a specific application. These processes or protocols were discussed in Chapter 2 when the OSI/RM was explained. As stated before, the OSI/RM establishes a framework for function standardization within protocol layers to facilitate modular protocol design. There is also some hope that the application specific services within the individual layers could some day be standardized. As an example, the International Standards Organization (ISO), is currently working on a file transfer, access, and management (FTAM) OSI File Service called Virtual Filestore. The objective of this work by the ISO is to define standards for transferring, accessing, and managing information stored in or moved between open systems as files. File attributes, file structures, and file operations are all listed and defined to provide a common model for file transfer on all systems. [Ref. 16: pp. 1414-1419]. Given the normal competition among various software, hardware, and network vendors, standardization at this level may well be an unrealistic goal.

However, standardization is certainly a better interoperability solution than the multi-vendor, heterogeneous, non interoperable file storage solutions we have now. Some standard services and procedures must be established to allow peer communications between the applications of two stations desiring to exchange information. This is the discourse that must be used to identify the services required for the application specified. File storage and retrieval, for instance, is not just the simple transmission of a serial bit stream to a given storage device then later reconnection to the same device to retrieve the same stream. Additional attributes like the file name, file protection, accounting information, etc, must also be stored and retrieved. A list of the files stored, the ability to delete or rename files, and moving files from one storage location to another are all examples of the many services used when storing or retrieving files. Based on the application, higher level protocols must select the services required, provide information needed by them, report errors in any of the interrelated processes as well as simply transmitting the data in the file. [Ref. 17: p. 1371].

Determining the services required by the user functional applications is not relegated just to the applications layer in the OSI/RM. Actually, the top four layers (application, presentation, session, and transport) all provide services (as described in Chapter 2) for every user application. According to Bartoli [Ref. 18: p. 196] these services can be common to multiple applications, application specific, or user specific. The common services, as you would expect, are used for information transfer by many applications regardless of their nature. Examples are set up and termination. Specific service elements satisfy the special needs of broad utility categories like file transfer, database access, job transfer, etc. User specific elements satisfy

particular user operations like word processing, computer aided design, etc. As the application progresses down the OSI/RM layers, more common and less specific services should exist. However, as we shall see in the interconnection section, multiple local and long distance network communications applications are the source of more special services. This increases protocol complexity in the lower layers of the OSI/RM. When compiled, the collection of all common and specific services required by the user functional requirements derived earlier is used to design and develop the protocols for the higher layers of the OSI/RM.

D. HIGHER-LEVEL PROTOCOLS

Once the necessary services have been determined, how are the protocols that support these services created? USMC programmers and engineers will not likely be writing protocols that support user applications or communications interfaces. However, we must develop expertise to evaluate vendor and standard protocols designed to support the services required by our users. Some sort of method is needed which enables those responsible for designing or evaluating large computer-based systems to determine exactly where certain specific protocol services fit within the general OSI/RM and whether they fit our needs. Our programmers are normally experts in specific subfunctions with limited knowledge of communications. This is true because defining interfaces between distributed software components takes more knowledge of the information to be exchanged than the media over which it travels. Reference manuals on what was done in the past are the common tool used by the system engineer to determine interface requirements. Bowers [Ref. 19: p. 479-487] describes a technique used by NASA which may be a better idea. This checklist technique identifies engineering considerations for interconnecting system modules on an electrical interface. This technique would

also be very useful for considering logical interfaces across protocol layer boundaries. The checklist is used as a guide to ensure that functions are not omitted and requirements are not underestimated. The following quote from [Ref. 19: pp. 479-480] describes the system for which this checklist technique was originally designed:

This system has several important characteristics. First, it is a large system managed by a number of organizational elements; second, it is very complex, comprising many elements with many interfaces; third, it is a distributed system, both geographically and in space; and fourth, it must be capable of evolutionary, modular growth, since replacement of the total system, whether to meet new requirements or to accommodate new technology, would be too expensive to contemplate. Clearly, some systematic approach is needed to adequately describe and document such a system.

This certainly fits the overall system architecture we are trying to design and evaluate. LANs are but one element, however, this kind of systematic approach will ensure that the LAN or any other technology chosen fits the needed services. Tables III-VI show the sequence of detail used by the NASA engineers to support and amplify the OSI/RM for their services and protocol applications.

The article indicates that a great deal of research was done to characterize NASA's needs as well as those of the general communications community. However, the work recommended by the first two sections of this chapter should provide the information needed to generate the USMC network specific tables. The ultimate objective here is to ensure user requirements are broken into a set of services defined more rigorously as they move down the protocol layers. Starting at the Application Level will ensure that each successive lower level protocol preserves the special characteristics of the higher level. It also makes sure that no lower-level services required by the higher-levels are omitted. The protocols in each layer can be viewed as

TABLE III
SUMMARY OF ASSOCIATION OF SERVICES WITH
THE OSI REFERENCE MODEL

Layer Services	Physical 1	Data Link 2	Network 3	Transport 4	Session 5	Presentation 6	Application 7
Electrical	-----						
Mechanical	-----						
Logical	-----	-----					
Address Management		-----					
Connection Life		-----					
Routing/Switching			-----				
Expedited Data							
Peer-to-Peer Layer Coordination							
Service Quality							
Flow Control							
Restart/Reset							
Management Reporting			-----		-----		-----
Multiplexing			-----				
Sequencing			-----				
Segmenting/Blocking			-----				
Format							
Gateway				-----			
Data Compression/Decompression						-----	
Encryption/Decryption	-----					-----	
Code Conversion						-----	
Virtual Device						-----	
Virtual Program						-----	
Syntax						-----	
Security			-----				-----
Cost Accounting			-----				-----
Priority				-----			-----
Scheduling				-----			-----
Semantics						-----	

TABLE IV
COMMUNICATIONS MODEL CHECKLIST GENERIC
SERVICES AND SUBFUNCTIONS

Services	Layer	1	2	3	4	5	6	7
Connection Life								
Establishment			X	X	X	X	X	X
Release			X	X	X	X	X	X
Abort				X	X	X		X
Multiplex operation			X	X	X	X	X	X
Initiation procedures				X	X	X		
Service quality matching				X	X	X		
Synchronization				X				
Routing/Switching								
Strategy					X			
Implementation				X				
Control node(s)				X				
Tables				X	X			
Cost					X			
Delay					X			
Congestion				X				
Scheduled/dynamic usage ..					X			
Priority					X			
Fail-safe/fail-soft				X		X		
Bandwidth allocation					X			

TABLE V

APPLICATIONS LAYER CHECKLIST

Security Identify logon and password requirements for:

- a) Access to the network
- b) Access to a remote host on the network
 - Identify multilevel security requirements and procedures for partitioning of resource access based on security level and passwords
 - Identify methods for initially entering logon ID and password into system tables and means for changing these entries by user and by system administrator
 - Identify means for reporting multiple attempts to enter passwords
 - Identify procedures for terminating connections that cannot satisfy password within reasonable number of tries.

Cost Accounting:

- Cost-account per connection for host and network separately
- Ability to change cost-accounts within a connection period.
- Verification of valid cost-account and permission to use cost-account.
- Reporting of cost-account use.

Priority:

- Priority for queue position, bandwidth allocation, minimum delay in use of network services, and ability to specify priority for host services.

Scheduling:

- Identify means for scheduling of host services, network routing, bandwidth, delay requirements, priority, security level during transmission, physical devices on hosts in support of application, and application program use.

Address Management:

- Application layer address is its legal cost account, logon ID, and password in each node or host.

Connection Establishment, Release, Abort:

- Establishment requirements based on logon ID, password, cost account, application program access password, and files access password.
- Release at normal program termination or programs error termination.
- Abort from programs at end or on receipt of manual abort signal from user.

Expedited Data:

- Ability of application program to generate a message having expedited priority.

Peer-to-Peer Layer Coordination:

- Coordination to ensure that sending and receiving devices and programs are available to send and receive data.
- All files are open and on-line and all supporting devices are operational and properly attached to required programs.
- Sufficient CPU, RAM, and other resources have been allocated.
- Any special parameter settings of the operating system or the application program have been made.

Communications Mode:

- Identification of interactive or batch requirement and initiation of programs in proper mode.
- Identification of any security requirements for encryption of fields and files or during actual transmission.

Quality of Service:

- Identification of specific generic parameters that can be employed by the Presentation layer to define bit-error rates, delay, lost data, restarts, bandwidth, and error reporting requirements.

Format Transformation:

- Hardcopy and softcopy format giving physical location of data fields, field sizes in lines and characters, color, shading, line drawing characteristics, font types, font sizes, hardcopy physical dimensions, interactive operator control fields (touch, lightpen, trackball, function key) relationships.

Semantics:

- Cause and effect relationships for interactive operations, error conditions in terms of programs to be initiated or services to be requested.

TABLE VI
ADDRESS MANAGEMENT

Application Address: Corresponds to the cost account and security identification used to verify the users legitimate use of the facilities.

Presentation Address: Corresponds to the file or physical device to be employed that may need format and syntax transformations for compatibility.

Session Address: To tie two software programs together. The duration of the session is independent of the duration of any other lower level support provided. The source and destination addresses appear as a specific bit string in a message for networks employing virtual circuits or datagrams. Normally equivalent to a port address or a virtual machine address.

Transport Address: To define a virtual circuit or communications channel between hosts or source and destination nodes on a network. This is independent of the number of physical devices at each host or node and independent of the number of intermediate nodes that support the communications link between hosts or the number of alternate or parallel paths between nodes and hosts. The address appears as a specific bit string in a message for networks using virtual circuits or datagrams (i.e., non-designated or unscheduled links). Normally equated to an end-node address (source or destination).

Network Address: To define a specific routing along one or more physical communication links between nodes within a single network having its own address structure. This address may be transparent to all layers above the network layer. It may or may not be required as a specific bit string by the network. For example, it is used to identify a table entry for the virtual circuit established between two or more nodes (source, intermediates, destination).

Internet Address: To define a specific connection spanning two or more networks, having their own address structure, within a larger national, international, or global network system. Employed only when communicating across several independent networks.

Data Link Address: To define a single physical connection between two nodes in a network. Parallel connections between the same two nodes have separate data-link addresses. Probably not a specific bit string in the message. Normally handled by flow control logic and circuit selection dynamics, and is known only to Network and Data-link layers.

individual data units meaningful in the layer to which they apply. Figure 3.3 [Ref. 20: p. 391] shows this relationship as it applies to the OSI/RM. The input generated by the user represents a set of instructions that must be packaged in one or more data elements and sent to another user or application. The application layer appends a header to accomplish the layer 7 encapsulation and passes the original user data plus the header to the presentation layer. At the presentation layer it is either preserved in its original data element size or broken into smaller elements each with its own presentation layer header. These headers will be used at the destination for regenerating the original application layer data elements. This process of data element plus layer unique headers continues down to the data link layer where the data elements are broken into frames and receive a header and trailer for transmission through the physical medium. When the frames reach the destination, the process is reversed. The header information is stripped off as the data elements move up through the layers arriving at the user in their original form and sequence.

The closer the lower-level protocols match the services requested by the higher-level application protocols, the more efficient the overall information flow throughout the network. This will also enable the information system to more closely mirror the special style and needs of a given organization rather than allowing the system chosen to force a change in the organization's information control strategy [Ref. 20: pp 390-391].

The first three sections of this chapter may all seem like an unnecessary academic aside but the need for identification of USMC specific requirements is critical. The keen competition for diminishing research, development, production, and operating funds mandates procurement of existing off-the-shelf network and processing components.

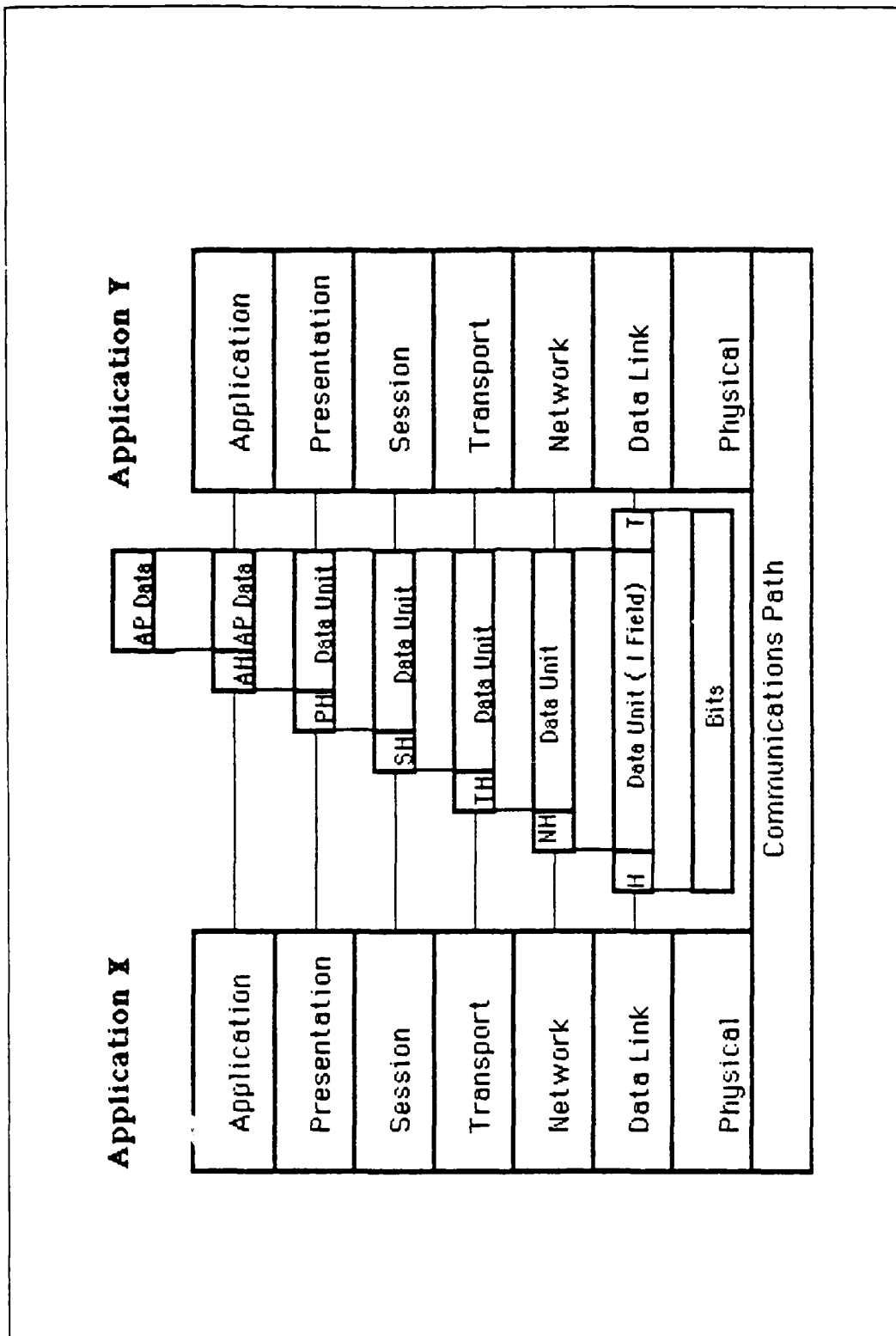


Figure 3.3 Protocol Layer Encapsulation.

This must be done to reduce development costs and allow economic logistics and maintenance support. It should not however, reduce our efforts to properly define our actual requirements. The extra up front effort will ensure that we get an information system that fits our needs. One that not only satisfies our user specific requirements but also does not have expensive unnecessary features accepted just because they were available. After the user requirements have been addressed local and long distance communications interconnection requirements are next.

E. INTERCONNECTION REQUIREMENTS

User networking requirements should be the next logical evolutionary step after application identification and information flow requirements have been specified. The ability to make the technology decision (i.e., LAN, CBX, shared processor, or a combination of all three) should be getting near.

As the capability of software packages on local networks grow to include distributed database management, electronic mail, text editing, file transfer, etc, so will the desire or need to expand the geographic coverage of the system providing these services. This will drive up the need for interconnection of local networks, either directly or through wide area networks. If not adequately addressed in the planning stages of local network design, the result will be efficient pockets of high speed data processing and data communications systems that are seriously degraded by inefficient slow interconnection solutions.

1. Local Network Interconnection

All computer networks are a collection of computing resources (hosts, terminals, communications controllers, servers, etc,) each of which can be viewed as a node. Nodes are connected by communications channels (physical and logical) which provide the paths to send and receive

messages. The node can be one or multiple hosts with associated terminals or an independently operated terminal not associated with a particular host. All terminals can connect directly to the host or may use communications processors or controllers along the way for connection to a particular host. A node could also be connected to the network to serve as a message handling node or gateway to an adjoining local or long distance network.

As discussed in Chapter 2, local networks are often distinguished from long distance networks by the area they cover and the speed at which they operate. Local networks are also oriented toward satisfying user information processing needs vice the long distance network orientation toward communications services. The benefits of the high speed local networks can be greatly diminished if interconnections are not minimized. However, when local networks require extension or connection, a bridge is the device used most often.

The bridge interconnects two logical local area networks using the same or different physical media but having common higher-layer protocols. It allows stations on different LANs to communicate as if they were on the same LAN. The bridge differs from a repeater because it is an intelligent filtering device used to store-and-forward frames moving between the LANs. The repeater is used only to interconnect cable segments on the same LAN. Figure 3.4 is an example of two local networks interconnected by a bridge. The bridge looks just like another station on each of the LANs but offers some very useful capabilities. The bridge in Figure 3.4 reads all the packets transmitted on LAN A accepting only those addressed to stations on LAN B. It receives each packet using the access protocol from LAN A, buffers the packets, then uses the appropriate protocols to access LAN B and pass on the traffic to the station on B

for which it was intended. It does the same thing for LAN B traffic going to LAN A. The bridge makes no modification to the content or format of the data in the packets.

LANs are limited by propagation delay, signal attenuation, and distortion (normally a function of the number of stations and distance to be covered). The bridge overcomes these problems by removing the traffic from the originating LAN then passing it to the destination LAN. This reduces the contention for access on each LAN and increases the number of addressable stations as well as the distance covered by the LAN extension. It also improves reliability because the loss of one LAN does not bring down all stations like it would if all were connected to the same LAN. It could add a security feature by creating a connection between classified and unclassified networks for passage of unclassified traffic only.

Special care should be taken when planning a local network strategy that employs bridges. The objective is to achieve high speed and high throughput connection between LANs thereby avoiding bottlenecks. Careful traffic studies, minimal differences in local network protocols, and adequate bridge buffer size will all help achieve this goal. Dissimilar local network interconnection or local network interconnection through long distance or wide area networks presents additional problems. These problems must be solved using more than a simple filtering pass through device like the bridge.

2. Local/Long Distance Network Interconnection

Long distance computer network interconnection is much like local to long distance voice telephone switching and terminal equipment networks. Local switches and networks use various unique features to enhance the services offered to local subscribers. Abbreviated dialing and conferencing are a couple of examples. However, when

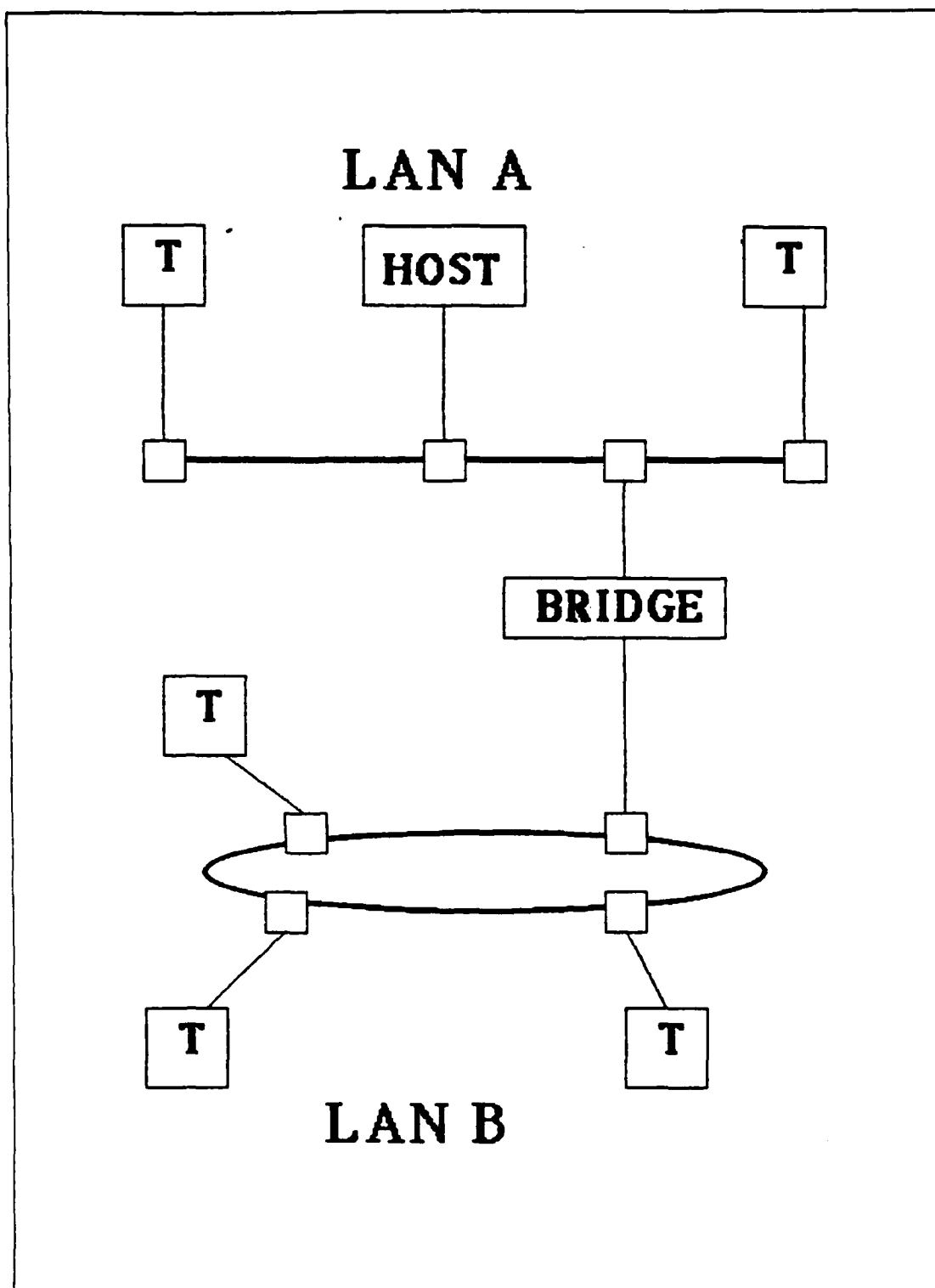


Figure 3.4 LANs Interconnected by a Bridge.

they desire to extend the connection outside the local area. they must adhere to standard physical and logical procedures for interconnection of their long distance calls. A common hierarchical structure of toll centers, primary centers, sectional centers, and regional centers work together with standard circuit switched voice oriented switching and transmission techniques to interconnect end offices which use centrally controlled star topologies. The long distance calls go only as high in the hierarchical structure as necessary for connection to the desired switch and ultimately the desired destination terminal. Calls are dynamically routed to control the flow and prevent congestion at individual switching centers or across individual links. Interconnection in a standard network like this presents few problems for the local network designer. He just follows the established network physical and logical design parameters for interconnection and transmission of his long distance traffic.

The long distance interconnection compatibility requirements for local computer communications networks is significantly more complex. The long distance telephone network evolved to its current refined highly compatible state over many years and offers local telephone network designers a stable standard set of design objectives and interface requirements. Local data handling networks have only recently evolved from independently developed often incompatible vendor network designs. As these networks grew in number, these same vendors developed their own long distance network switching and transmission architecture or simply used those employed in their mainframe time-shared computer configurations. These architectures were specifically designed to handle traffic generated by equipment and protocols unique to their own individual designs. The communications services and protocols used were also

specially designed to offset problems unique to long distance networks. Like the long distance telephone system, long distance data networks are inherently less reliable due to the effects of noise generated in long distance transmission media. Changes from one format to another depending on the network or link used also contribute to this problem. Because of the distances involved and diversity of communications channels used (telephone, leased line, satellite, and microwave) getting bandwidth for high speed service is an expensive proposition. Therefore, complex switching and protocol techniques are used to maximize the efficient use of this expensive commodity called bandwidth. They also try to offset the network reliability problems. Switching, encapsulation, fragmentation and reassembly, connection control, flow control, error control, synchronization, sequencing, addressing, multiplexing, and transmission services are all examples of parameters used to route traffic, to improve reliability, or to offer special services [Ref. 20: pp. 375-385]. One or all of these parameters can differ depending on which long distance network is selected.

This presents a classic conflict of interest between local and long distance networks. The long distance network uses complex protocols that sacrifice processing time to reduce bandwidth requirements and effectively use channel capacity. Local networks, on the other hand, use simple protocols that waste channel capacity to reduce processing time [Ref. 21: p. 71]. Interconnection of these two diverse network protocol sets is done by using a translation device called a gateway. The gateway is more complex than the bridge device previously described because of the many differences between local and long distance network protocols. Addressing schemes, packet sizes, network interface protocols, time-outs, error recovery techniques, status

reporting procedures, routing techniques, access controls, and connection or connectionless service all represent differences the gateway may be designed to resolve [Ref. 22: pp. 168-169].

The layered protocol architectures of the OSI/RM and INTERNET Model (developed from ARPANET experience) were discussed in Chapter 2. Digital Equipment Corporation (DEC) Digital Network Architecture (DNA) and IBM's System Network Architecture (SNA) offer two additional protocol architectures used in today's long distance networks. Figure 3.5 shows how the SNA and DNA protocol architectures match up against the OSI and INTERNET model architectures. The following amplifies the functions of the DNA and SNA architectures.

a. Digital Network Architecture (DNA)

DNA uses a strong protocol layering with a data link control level, a logical connection or virtual circuit, and a user application-level much like ARPANET. The network service protocol (NSP) is a lot like the transport protocol in ARPANET but DNA does not distinguish between host computers and switching nodes (IMPS in the ARPANET). Some of the DNA system nodes run user programs, some switch packets, and others do both. DNA is divided into the five function layers (Figure 3.6).

(1) Physical Layer. The physical layer performs the same functions as the physical layer of the ISO OSI/RM described in Chapter 2. Electrical characteristics like clocking, signalling, and carrier service interfaces are the functions of this layer.

(2) Data Link Control Layer. This layer uses a DNA unique protocol called digital data communications message protocol (DDCMP) to create a sequential error-free communications path between adjacent nodes for the transfer of data blocks.

OSI		INTERNET		SNA		DNA	
1	APPLICATION	1	PROCESS/ APPLICATION	1	FUNCTION MANAGEMENT	1	USER
2	PRESENTATION	2		2	DATA SERVICES	2	NETWORK APPLICATION
3	SESSION	3	HOST-HOST	3	DATA FLOW CONTROL	3	NETWORK SERVICES PROTOCOL
4	TRANSPORT	4		4	TRANSMISSION CONTROL	4	
5	NETWORK	5	INTERNET	5	PATH CONTROL	5	TRANSPORT
6	DATA LINK	6	NETWORK ACCESS	6	DATA LINK CONTROL	6	DATA LINK
7	PHYSICAL	7		7		7	PHYSICAL

Figure 3.5 Communication Protocol Architecture Comparison.

(3) Transport Layer. This layer is used for transporting messages from the source to the destination node. It uses a route table and routing algorithm to provide an adaptive scheme for end-to-end path establishment through intermediate nodes. It is highly dependent on the Network Services layer for path establishment.

(4) Network Services Layer. This layer uses NSP to create and manage the logical path between users. With the help of the transport layer it uses flow control and buffer management to uniquely route each packet then reassemble them at the destination.

(5) Application Layer. Application functions for services like file transfer, terminal control, database transaction requests, and data transfers program-to-program are accomplished through independent logical links at this layer.

b. System Network Architecture (SNA)

IBM also uses a layered protocol architecture (Figure 3.7). This architecture is oriented toward secondary terminal nodes accessing a single or small number of primary main computer nodes rather than equally capable nodes connecting on equal footing. All of the layers can reside on the host or link path controls can be taken off the host and handled by software in a separate communications controller. Path access can also be handled outside the host by a separate front-end processor. The user gets a sequential serial bit stream making the network appear transparent regardless of the topology, route, or transmission media used. Network addressable units called sessions establish logical connections via the SNA protocol layers.

(1) Data Link Control Layer. This layer uses a unique Synchronous Data Link Control (SDLC) protocol to package and transmit the data bitstream from the higher layers on the point-to-point or multi-point switched or

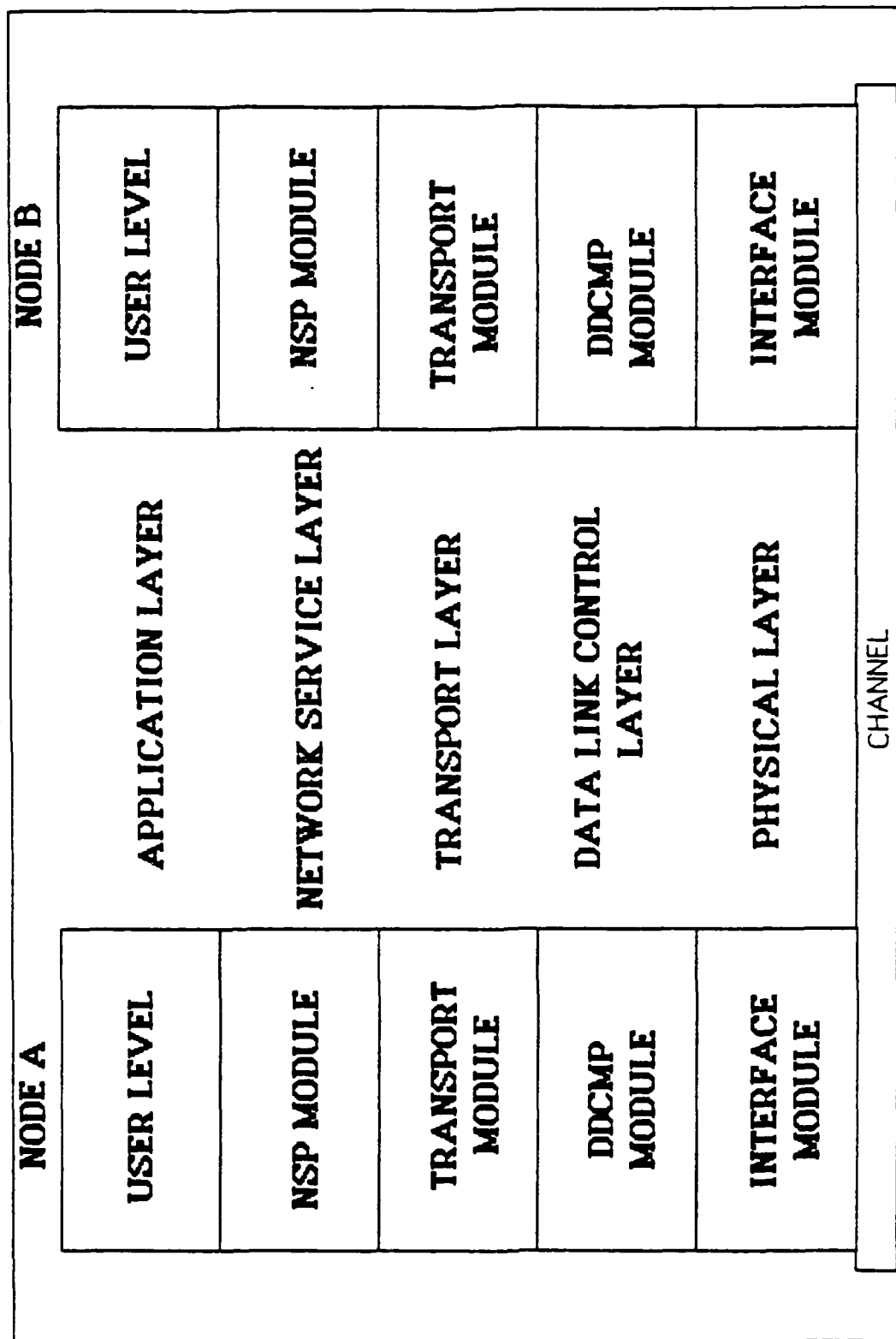


Figure 3.6 DNA Protocol Architecture.

non-switched connections. SDLC is totally transparent to the higher protocols and does not attempt to interpret any of the data structures coming from them. It simply uses its own packaging and control structure to pass the raw data error free.

(2) Path Control Layer. The path control layer controls congestion by dynamic packet routing in the communications subnetwork. It can improve efficiency by packetizing outgoing messages and depacketizing incoming messages.

(3) Data Flow Control Layer. This layer carefully matches varying types of input from different users to ensure user request/response flow and flow integrity are maintained. Selecting full duplex or half duplex, user modes, and message grouping are all examples of the services offered by this layer.

(4) Presentation Services Layer. Data transformations, additions, and editing functions are performed in this layer to ensure the data is in the proper format for terminal presentation.

(5) End User Layer. Each network element that can send or receive data is assigned a network address and is known as a network addressable unit (NAU). The network address uniquely identifies the element regardless of whether it is a device (terminal or terminal control unit), a program (like an application program in a cluster controller or host processor), or a part of an SNA access method. The network address contains the information necessary to route data to its destination. A hierarchy of domains exist for network control and each domain is controlled by a System Services Control Point (SSCP). These SSCPs communicate with each other in the overall management of the network.

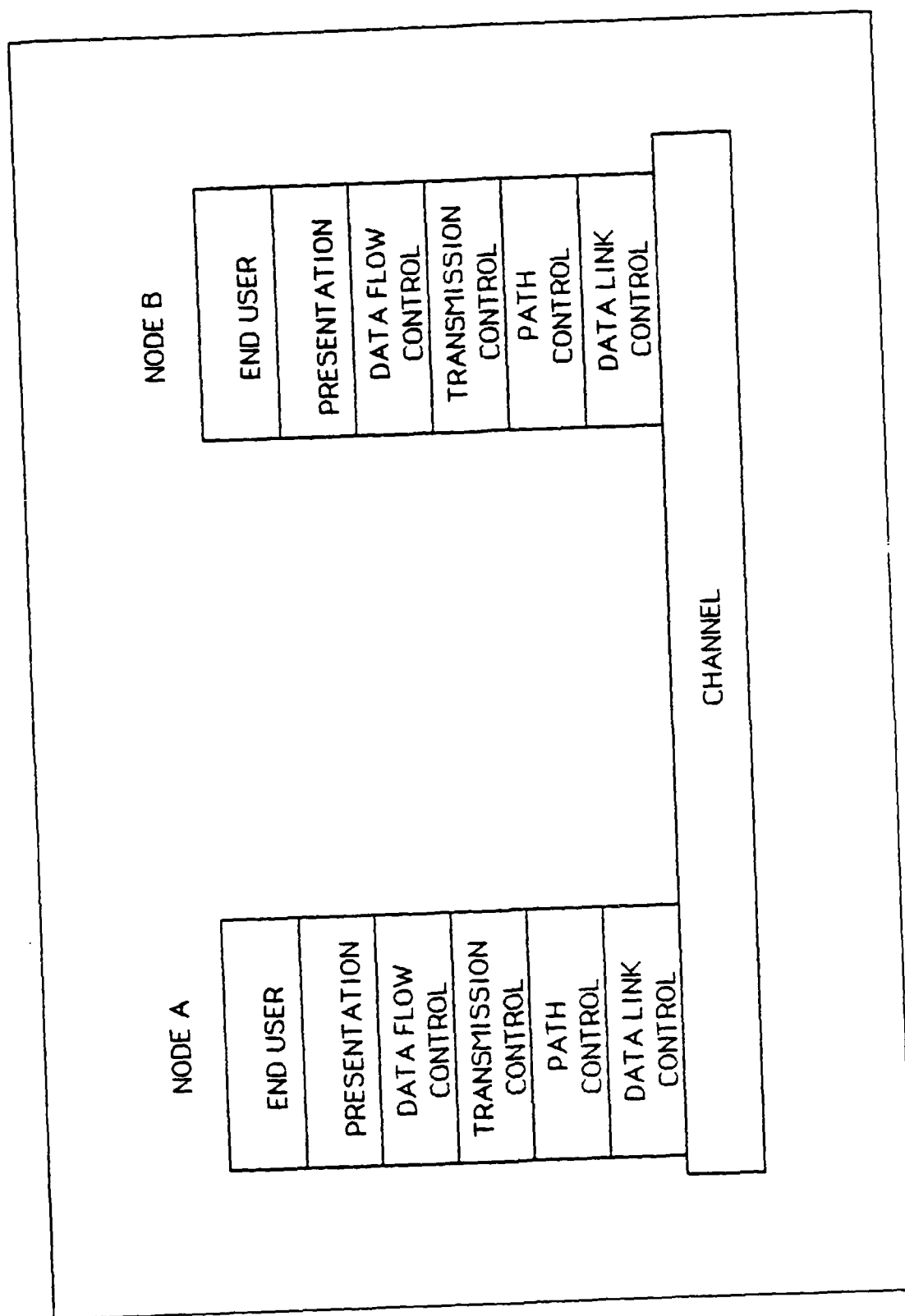


Figure 3.7 SNA Protocol Architecture.

3. USMC Local/Long Distance Network Strategy

A little over 6 years ago, when the ARPANET (later the DOD INTERNET) model had not yet matured, the U.S. Marine Corps was given permission to build an interim temporary long distance data network. This network was designed to satisfy data transmission and communication requirements between mainframes at several Marine Corps installations. The result was the Marine Corps Data Network (MCDN) (Figure 3.8). Table VII-IX provide the breakdown of hosts, FEPs, sub areas, site IDs, and trunk group identifiers that correspond to the the Figure 3.8 numbers and letters.

MCDN is a common-user, data communications network which provides terminal-to-computer and computer-to-computer communications for all functional Marine Corps Automated Information Systems (AIS). It is primarily designed for the supporting establishment and Fleet Marine Force units in garrison. Since the mainframes were IBM, SNA was the logical choice for the local and long distance protocol architecture. This architecture is based on the use of communications processors (NCR COMTENS) as the major nodal elements in the network. All terminals connected to the network are given access to any host computer in the network in an on-line interactive mode. Connectivity between nodal points in the MCDN is provided by leased commercial telephone circuits. The communications processors perform the following specific functions:

- Front-end processing for all host computers
- Switching/line control for all terminals
- Network communications functions

All computer terminals and remote job entry (RJE) work stations gain access to MCDN via dedicated/dial-up circuits to the nearest communications processor. Extensive use of terminals served by polled, multi-drop circuits are used to minimize circuit costs while facilitating interactive terminal-to-computer communications.

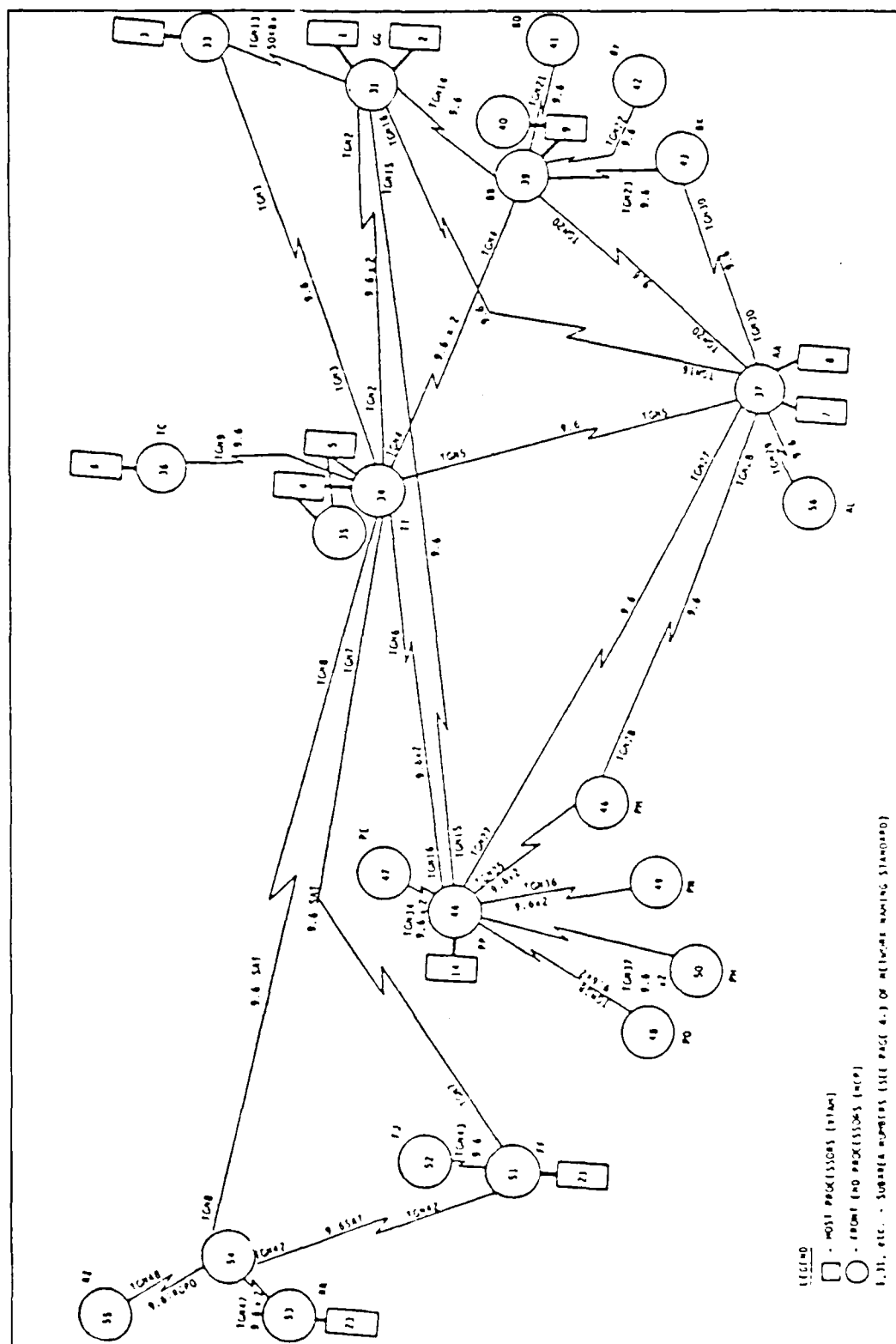


Figure 3.8 Marine Corps Data Network (MCDN).

TABLE VII
MCDN DESIGNATIONS

<u>REGIONAL CONTROL NODE</u>	<u>SUBNODE</u>	<u>MCDN DESIGNATOR</u>
MCCDPA ALBANY	4TH MAW (NEW ORLEANS)	ALA NOL
RASC CAMP LEJEUNE	FMFLANT (NORFOLK) MCRD PARRIS ISLAND RASC CHERRY POINT	CLB NFD PIK CPY
RASC HAWAII	MCAS KANEOHE BAY	HIF KBJ
MCCDPA QUANTICO	HQMC	MQG HQI
RASC CAMP PENOLETON	RASC EL TORO MCAS YMA MCLB BARSTOW MCB 29 PALMS MCRD SAN DIEGO	CPP ETE YMH BAM TPN SDO
RASC OKINAWA	RJE CAMP FOSTER MCAS IWAKUNI	OKR OKQ IWZ
MCCDPA KANSAS CITY	MCRSC OVERLAND PARK	KCT RFC

TABLE VIII
MCDN SUBAREA ASSIGNMENTS

<u>NODE</u>	<u>HOSTS</u>	<u>NCPS</u>	<u>LOCATION</u>
HQG	1-2	31-32	QUANTICO
HOI	3	33	HEADQUARTERS
KCT	4-5	34-35	KANSAS CITY
RFC	6	36	RESERVE FORCES
ALA	7-8	37-38	ALBANY
NOL	26	56	NEW ORLEANS
CLB	9-10	39-40	CAMP LEJEUNE
NFO	11	41	NORFOLK
CPY	12	42	CHERRY POINT
PIK	13	43	PARRIS ISLAND
CPP	14-15	44-45	CAMP PENDLETON
BAM	16	46	BARSTOW
ETE	17	47	EL TORO
SDO	18	48	SAN DIEGO
TPN	19	49	29 PALMS
YMH	20	50	YUMA
HIF	21	51	CAMP SMITH
KBJ	22	52	KANEOHE BAY
CKR	23	53	CAMP KINSER
OKQ	24	54	CAMP FOSTER
IWZ	25	55	IWAKUNI
	MAF	61	
	SRM	62	

TABLE IX
NODE ID, DESTINATION ID, AND LINE NUMBER

<u>NODE ID</u>	<u>DEST ID</u>	<u>NODE AND LINE NUMBER</u>
TTNJE04, TTNJE05	KANSCITY	20
GGNJE01, GGNJE02	QUANTICO	22
GINJE03	HQMC	24
AANJE07, AANJE08	ALBANY	25
PPNJE14, PPNJE15	CAMPEND	27
PMNJE16	BARSTOW	29
PENJE17	ELTORO	30
PONJE18	SANDIEGO	31
BBNJE09, BBNJE10	CAMPLEJ	32
FFNJE21	CAMPSMITH	33
RRNJE23	CAMPKIN	34
BYNJE12	CHERRYPT	35
BKNJE13	PARRISLE	36
RZNJE25	IWAKUNI	37
TCNJE06	RESSUPCT	38
BONJE11	NORFOLK	39
RCNJE24	CAMPFOST	40
FJNJE22	KANBAY	41
PHNJE20	MCASYUMA	42
PNNJE19	29PALMS	43
ALNJE26	NEWORL	44

MCDN provides a responsive reliable synchronous time division multiplexed circuit switched long distance data transmission service for the many users at each site. However, now that DDN has been designated as the official long distance data network for all of DOD, the Marine Corps is attempting to transition to DDN for long distance connectivity. The Marine Corps and the Defense Communications Agency (DCA), in conjunction with several prime and support contractors for both networks, are attempting to develop and test an efficient protocol conversion technique which will permit this transition. A five phase test and evaluation effort began in November 1985 to address the following issues:

- IBM SNA architecture compatibility with the DDN
- Sub-network management
- Network diagnostics
- Remote initial load of remote processors
- Response times as guaranteed by DDN system specifications
- Dedicated packet switched node (PSN) resources

The test was designed to gradually build from a single pair of nodes, testing the basic interface, to multiple nodes testing the connectivity with actual operational traffic loads.

a. Phase I

This phase, conducted in January 1986, was used to gather statistics like host utilization, line utilization, response times, and throughput on the current configuration being used by MCDN. This baseline data will be used as a benchmark for comparing the performance of the MCDN in its current leased line configuration versus the DDN.

b. Phase II

The configuration in Figure 3.9 will be used in Phase II, March 1986, to ensure that a session can be

established and maintained through the DDN. A COMTEN processor currently being used for local processing at Kansas City, Mo., will be used to test the newly developed NCR COMTEN X.25 and Communications Network Service (CNS) software. This new software will be exposed to the operational DDN environment for the first time during this test.

c. Phase III

The configurations in Figure 3.10 will be used during Phase III, April 1986, to establish the optimal equipment configurations for DDN connectivity. Initially, only Kansas City and Quantico will be connected then Albany, Camp Lejeune, and Camp Pendleton will be brought on line.

d. Phase IV

Phase IV, May 1986, will simulate MCDN in an operational mode with DDN using the configuration established during Phase III. The same statistics collected during Phase I will be collected during this phase for comparison.

e. Phase V

Phase V, June 1986, will be used to analyze test results and produce a test report.

The results of this test will have a significant impact on how the Marine Corps plans to provide future long distance connectivity to local subscribers. The decision on how this will be done also impacts decisions on local network protocol specifications. Will the Marine Corps continue to think in terms of the centralized IBM mainframe configurations used now? Will local networks be connected through these hosts which are in turn connected through DDN as shown in Figure 3.11? Maybe test results will show that this is not an efficient reliable solution. This may leave local networks connected through the IBM hosts which will continue to be connected through MCDN (Figure 3.12). Will the entire centralized processing philosophy soon change to

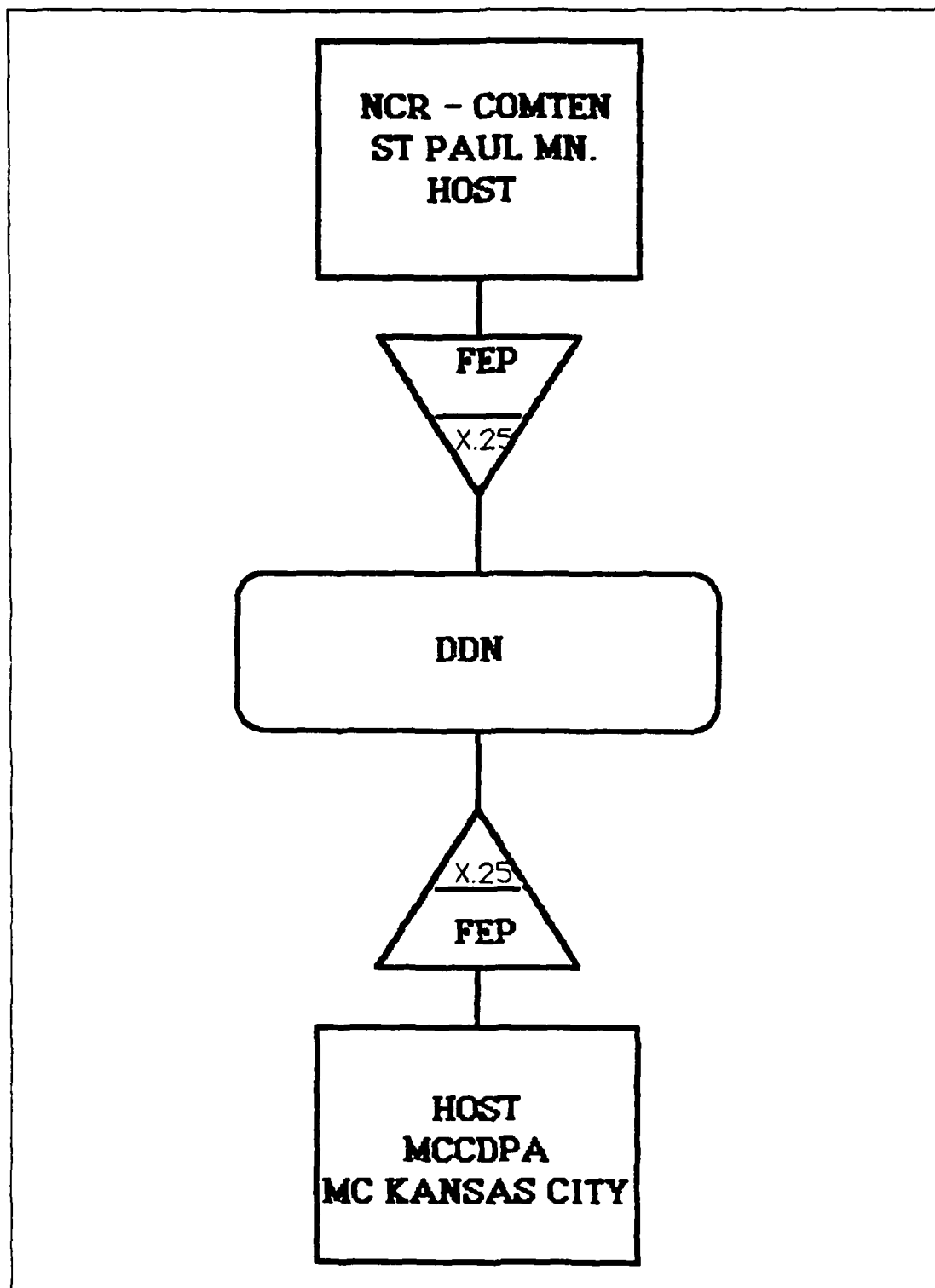
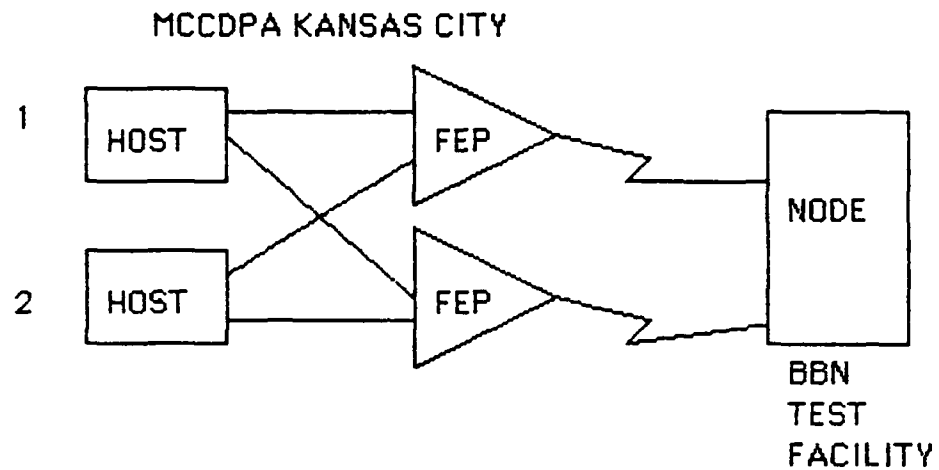


Figure 3.9 Phase II MCDN/DDN IPR.

A FUNCTIONALITY TEST



B

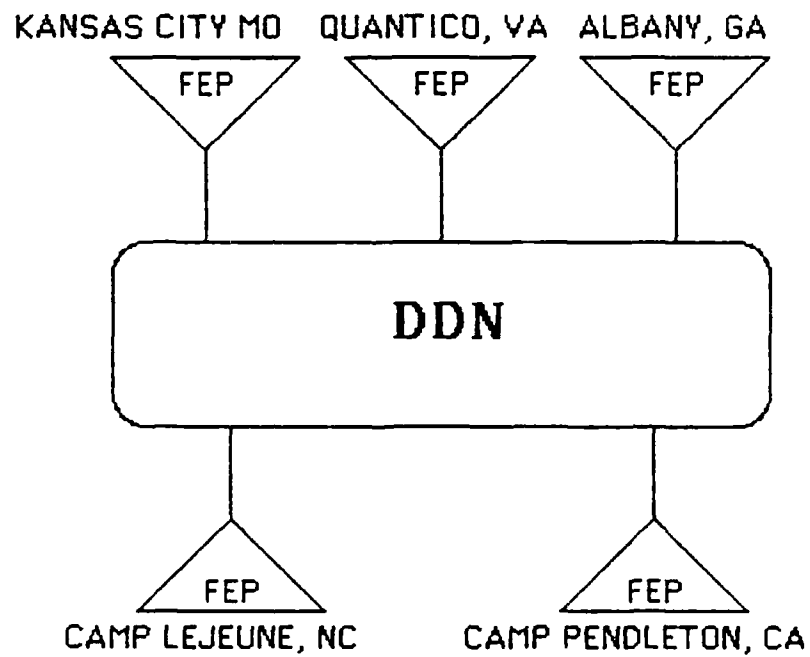


Figure 3.10 Phase III MCDN/DDN IPR.

a more distributed perhaps asynchronous approach as depicted in Figure 3.13? If so, should the SNA synchronous protocols be forced upon all local networks? Can third and fourth generation CBX's with associated wideband digital trunking capabilities be considered for use as bridges and gateways for local as well as long distance connectivity? Will public switched packet data networks be used for future long distance connectivity as shown in Figure 3.14? If so, which ones and what protocols do they use? These and many more questions must first be answered in order to develop an overall network strategy. This will ensure that unnecessary expensive connections, bridges, gateways, and protocol conversion requirements are not imposed on the all LAN specifications just to cover all contingencies.

Identification of the location and type of information sources outside the local area allows identification of the long distance network best suited for long distance interconnection. Since most of the traffic is local, these parameters may not be the driving force in local network access and communications strategies but they cannot be ignored. This reduces the chance of selecting a local network strategy that is rendered woefully inefficient or even worse cannot pass traffic when connected to a long distance network.

Common layer separation and functional responsibility assignment was the intent of the OSI/RM and the DOD INTERNET concepts. However, the previous existence or concurrent development of network solutions like IBM SNA and Digital Equipment Corporation (DEC) Digital Network Architecture (DNA) resulted in public long distance data networks that use different protocols. In the case of MCDN and DDN, military long distance data networks that use different protocols for encapsulation, switching, and transmission also exist. The Marine Corps must develop an

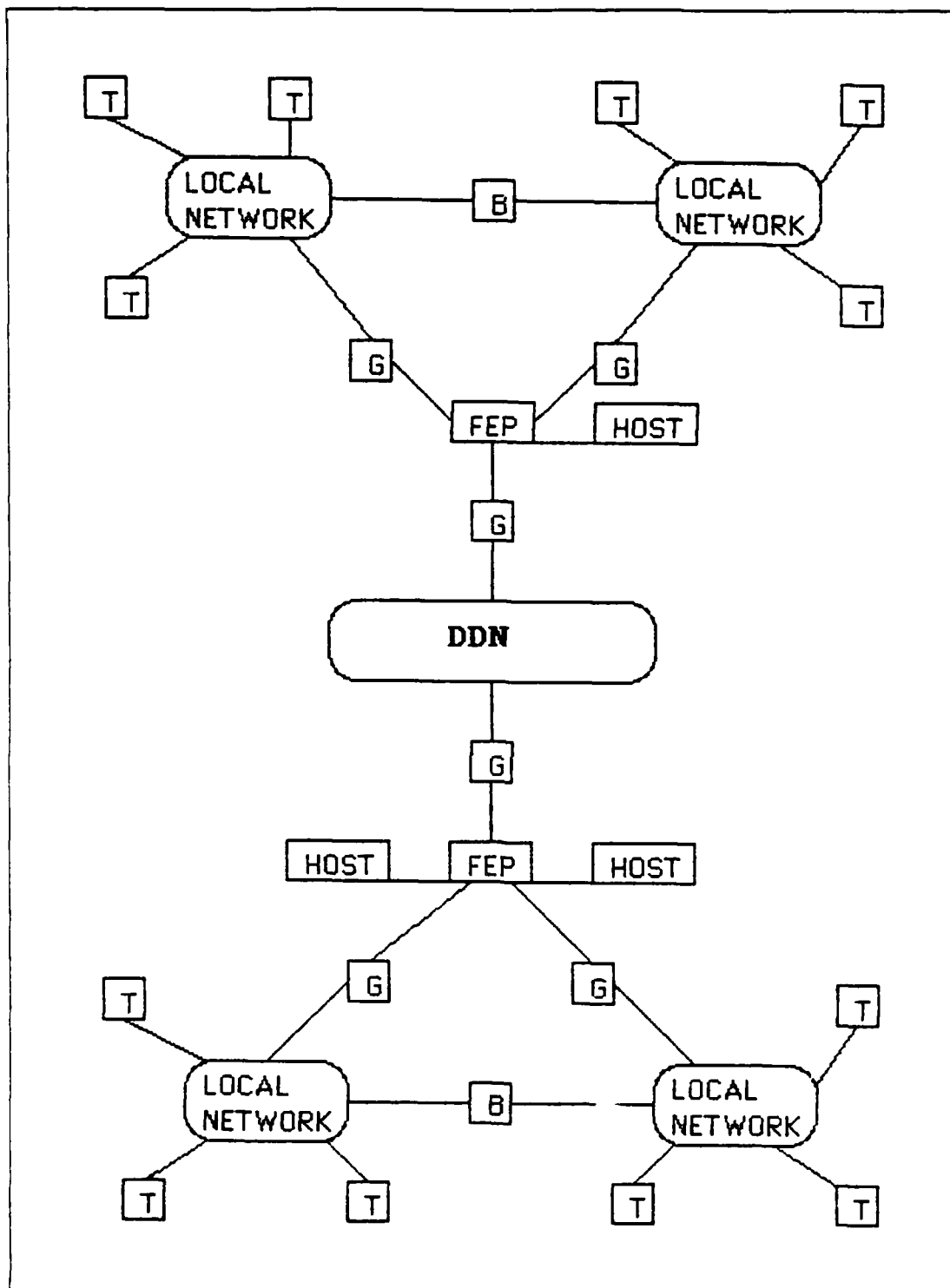


Figure 3.11 Local Networks Connected
Through MCDN Hosts and DDN.

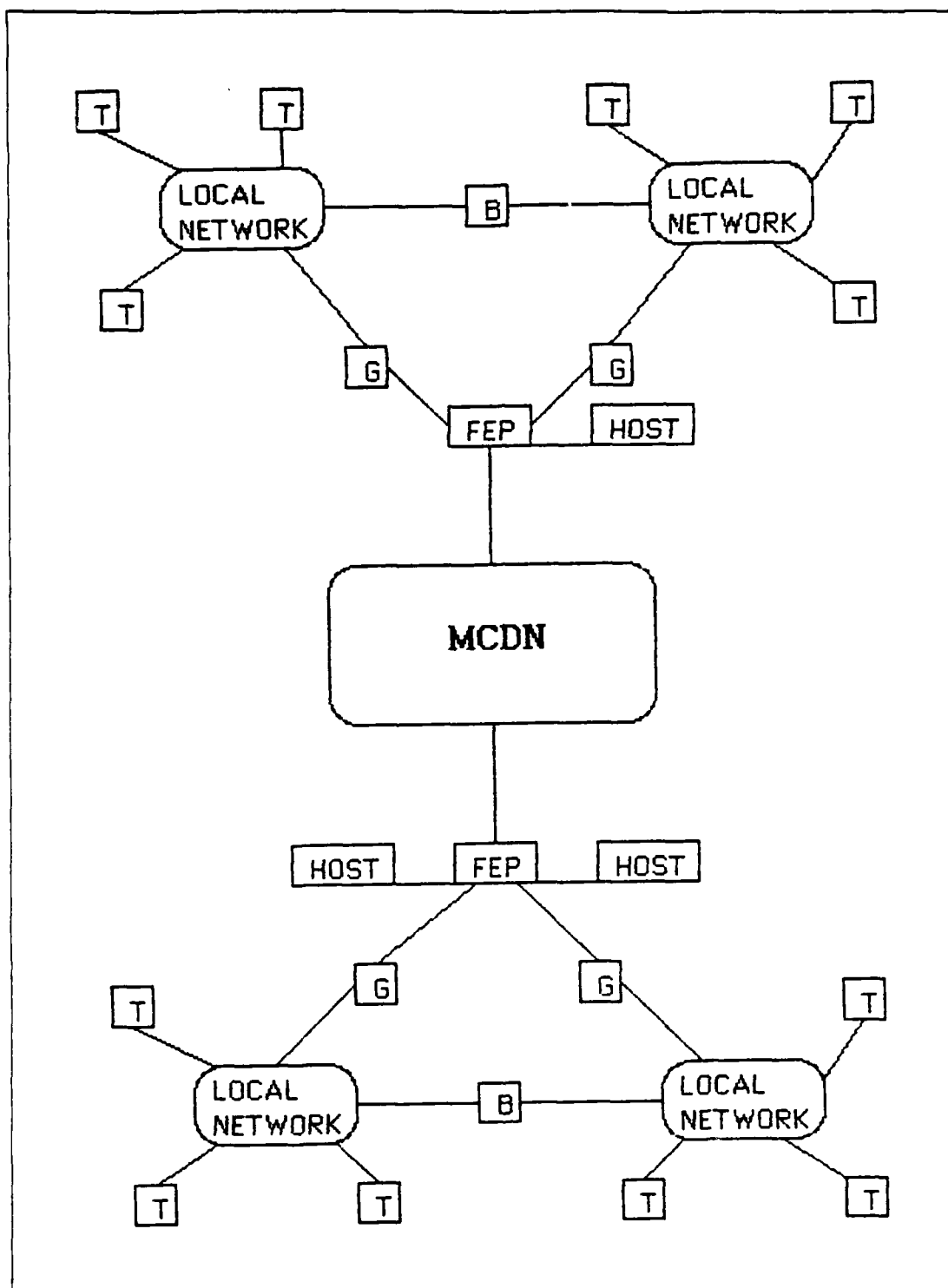


Figure 3.12 Local Networks Connected Through MCDN Hosts and Network.

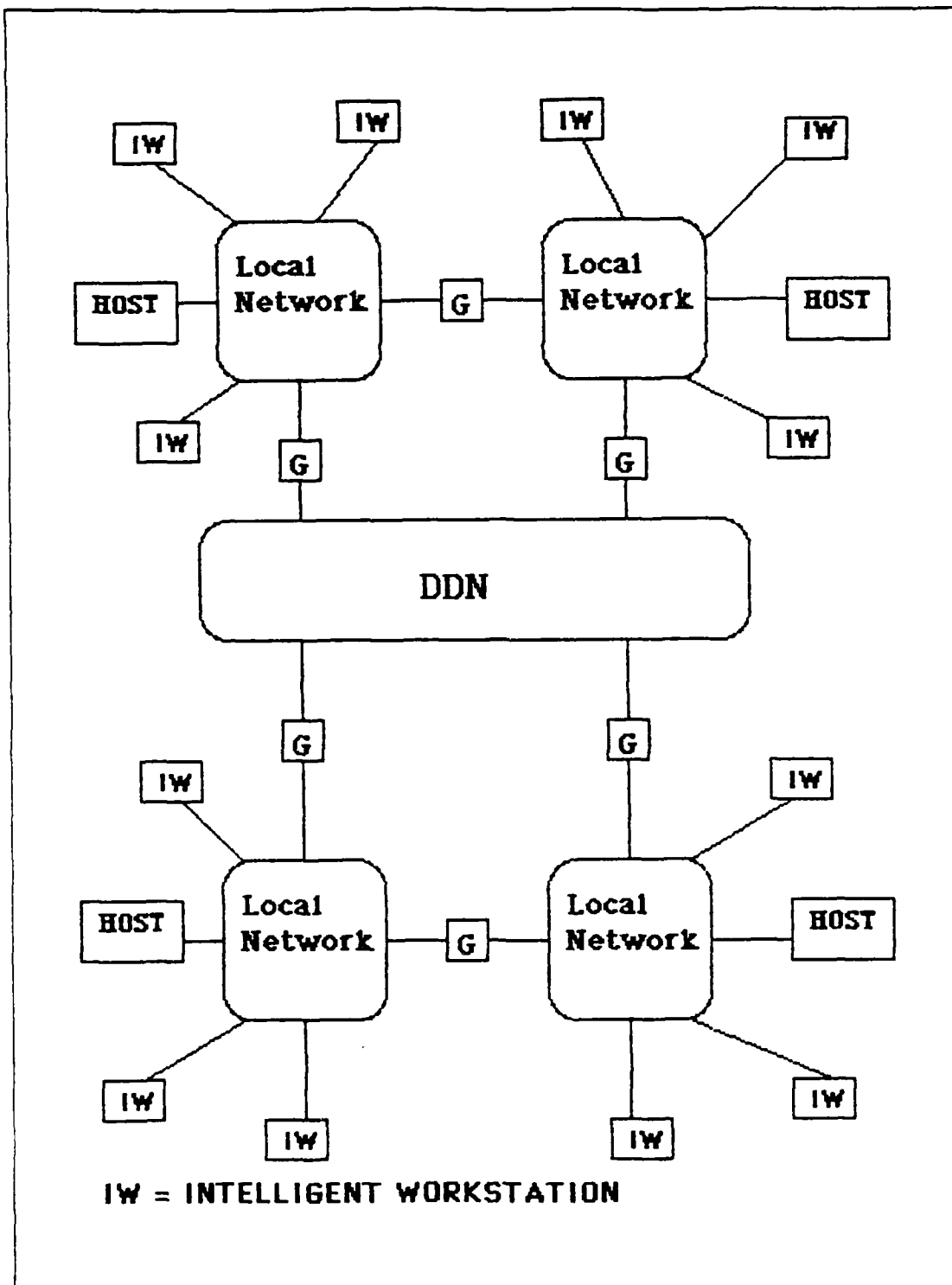


Figure 3.13 Local Networks With Distributed Processing Connected Through DDN.

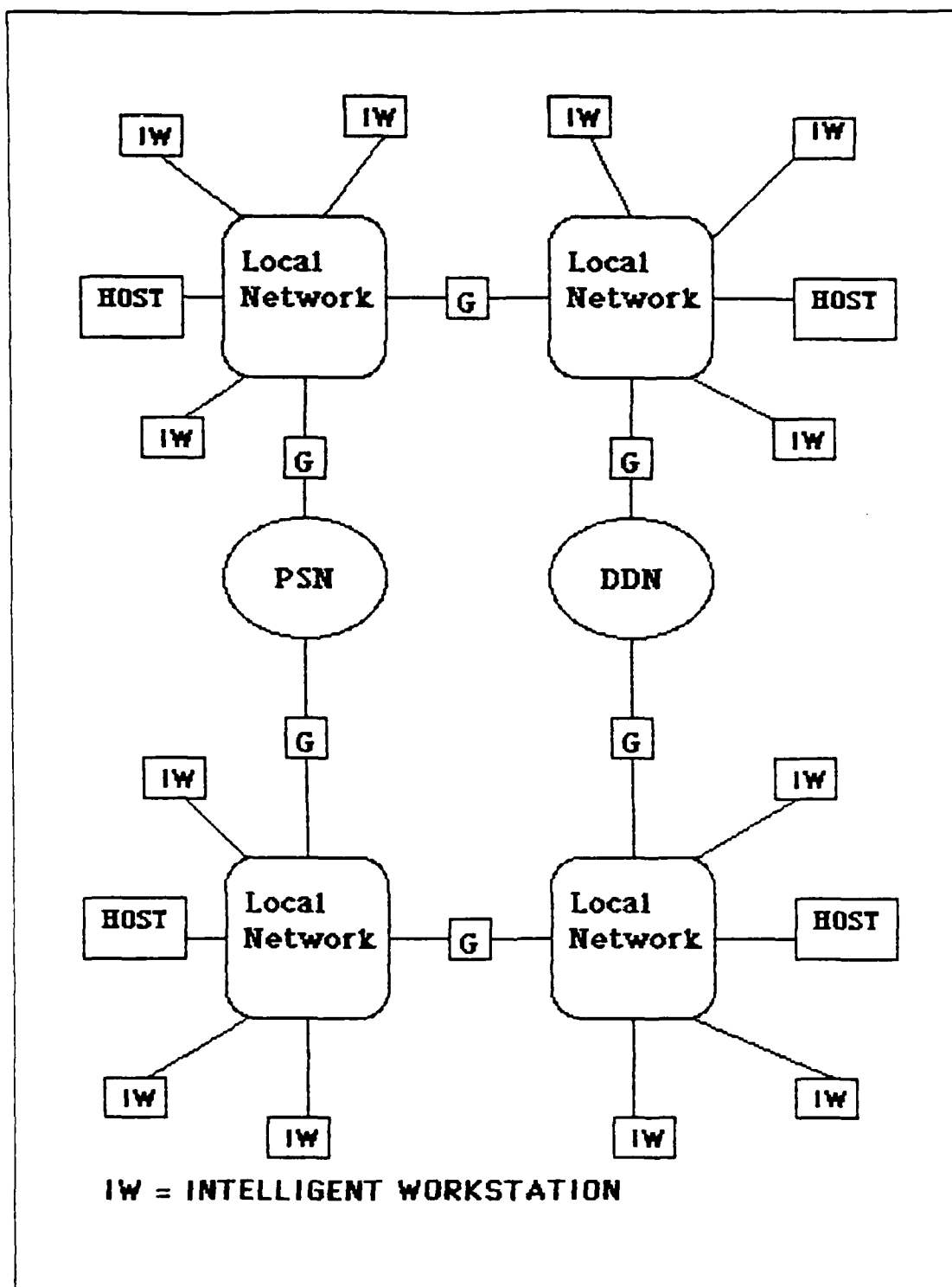


Figure 3.14 Local Networks With Distributed Processing Connected Through DDN and Public PSN.

overall local/long distance network strategy. This will lead to choosing only one network for long distance interconnection or the adoption of multiple translation and mapping protocols within all local networks. The fact remains that local networks will be influenced by the protocols used in already established and emerging long distance networks. Hard decisions must be made.

After careful consideration of user requirements translated into services and higher-level protocols as well as long distance network interconnection requirements, a LAN may well be the technology selected to satisfy the local network requirement. This only begins the specification process. Numerous other performance oriented operation and management requirements must be included.

F. LAN SPECIFICATIONS

1. General

Coordinated cooperation between user, network designer, and contracting specialists is never more critical than during the specification process. What you get in vendor proposals to satisfy actual requirements is only as good as the detail and completeness of the specifications prepared for the solicitation package. Vague, general, and basic specifications just give the vendor an opportunity to submit an abundance of detail on the features of his own system without ever having to translate those features into required operational performance capabilities. To this point, the LAN specifications have been oriented toward satisfying user requirements.

The information collected, analyzed, and used to determine services required should provide answers to the following (among other) questions:

- What kinds of applications and services will be needed?
- What are the transmission types and throughput requirements?

- Is there a need to integrate services and if so which ones?
- How many sites and what distances will the LAN cover?
- Are there any special data transfer requirements?
- What types of computing and communications devices (computers, printers and print spoolers, file servers and disc drives, plotters, modem servers, emulators, etc,) must be handled by the network?

The information gathered, the answers to these questions, and the local and long distance connectivity considerations were used to make the LAN technology decision. The latter also introduced the first of the many support considerations that have an affect on the LAN specifications. The local and long distance connectivity identified the network interface requirements (gateways, bridges, hosts, etc,). This information can all be directly translated into LAN specifications. However, there are still many unanswered questions like:

- What are the future growth requirements?
- Who will install, support, and maintain the network equipment?
- What type of network management scheme will be used and what functions must it have?
- Are there any other special constraints or requirements like priority, precedence, reliability, availability, security, etc?

2. Performance

Several general software and hardware characteristics can be added to the specific needs already stated. "User friendly" is a much used term that characterizes the desire and sometimes fear of every non technically oriented user about to acquire a new and unfamiliar system. The state of technology today permits the system, software, and hardware designers to give users special features. These features offset the technical complexity of the new sophisticated systems. User guides and manuals, directories of network services, and online menus to guide the user through complex operations are all examples of techniques used to

increase user friendliness. Plans for how operating characteristics, capabilities, and limitations of the new system will be introduced to prospective users is a critical part of system specification and acceptance. Knowledge of how the vendor's proposed network will create new or change existing system command, planning, engineering, execution, control, and coordination procedures opens the door for adequate user preparation. If necessary, users are more willing to provide input on tradeoffs that might have to be accepted for other critical performance features. By making the user a part of this decision process, he will be more inclined to accept and help resolve future system shortcomings and problems.

LAN throughput is directly related to the transmission medium, access method, processing capacity at each network node, and, as stated before, the amount of protocol translation required for interface variations. A detailed quantitative traffic analysis would be most useful for the specification document. Traffic types; message size, integrity, sequencing, and accountability; link speeds; number of connections; response times; etc; can all be used to give the vendor accurate and specific throughput speed requirements. Stringent reliability requirements in command center type operations can also contribute to this specification element. Several of the ongoing government funded network modelling and traffic handling analysis projects may prove to be an invaluable source for appropriate future throughput numbers.

The request for flexibility in the specification may seem trite but there must be some insurance that the system will be kept modern as user requirements change. Modular design techniques will ensure that the entire system does not require replacement all at once. Commercially available software tools ensure supportability.

AD-A168 861

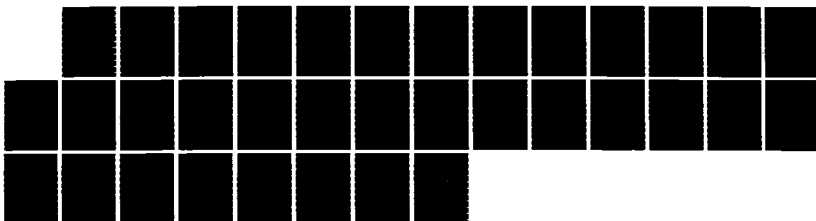
LOCAL AREA NETWORK STANDARDS AND GUIDELINES FOR US
MARINE CORPS APPLICATIONS(U) NAVAL POSTGRADUATE SCHOOL
MONTEREY CA T J HINES 27 MAR 86

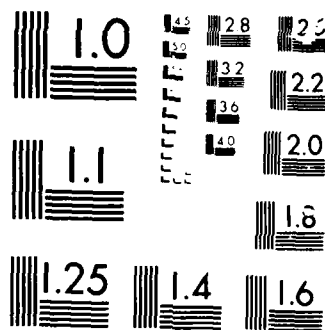
2/2

UNCLASSIFIED

F/G 17/2

NL





Contractual flexibility is the key to substituting modern components during the life of the contract. This may be the key to future network growth to handle features and services like video teleconferencing, artificial intelligence for automated decision aides, common user reference databases, speech recognition for voice mail and dictation, integrated voice and data plus many more.

3. Facilities/Support

Overlapping development, training, manpower, operations, logistics, and maintenance costs result in life-cycle resource requirements which cannot be supported. This is especially true for manpower which is the most expensive element. Therefore, we should use technology to reduce manpower intensive operations within any information system architecture. Simply substituting newer versions of existing physical systems or even worse adding additional systems is not the solution. Technology that can reduce costs include: embedded intelligence consisting of built-in test equipment, fault detection, isolation and restoral, fault-tolerant design, and artificial intelligence (expert systems); portable/reusable software to reduce development and maintenance costs; throw away maintenance to reduce logistics support costs; and finally centralized operations and maintenance to reduce manpower requirements. Early identification of manpower intensive operations in existing functional mission requirements and explicitly stated operations and maintenance requirements (capabilities and deficiencies) in the requirements documentation will facilitate potential savings opportunities.

Organizations use various approaches to management and control of resources. Most military organizations have a highly centralized, hierarchically structured, formal chain of command while some are more decentralized. Those thinking about putting together an information system

architecture that uses LAN technology should realize that they imply a more distributed approach to sharing information. A key issue is support for these distributed services. Organizations with highly centralized resources and well defined support procedures (software and hardware development, maintenance, operations, etc,) may not be able to support or control a LAN environment. This is an environment where powerful personal computers are physically separated and interconnected to database managers and servers. Proper characterization of this new environment would provide specific well defined functional control and support procedures. It is these procedures that are used to specify and evaluate potential network technical/performance, processing, communications and maintenance features as well as hardware configurations.

The paucity of funds for future operations will not permit a separate maintenance support contract for every LAN installed aboard a base. Yet, as users become more familiar with and dependent upon technologically improved data systems, they will impose increasingly more strict requirements on them. Like the current telephone system, these new systems will be expected to be available 24 hours a day, 7 days a week [Ref. 23: p. 5-6]. Who will provide the day-to-day maintenance and network control support for LANs? Base and Station Communications Electronics Officers (CEO) already feel strapped for people to maintain existing cable plant and switching equipment. In addition, the current feeling among many CEOs is that LANs are data processing systems that should be operated and maintained by those who own them. Marine Corps data processing facilities have the experience in network management of computers and computer communications networks (MCDN). However, they too contend that they don't have the people nor the desire to support LANs not directly associated with their own data processing

facilities. Will computers and data communications someday become so commonplace that every organization has someone capable of administering, managing, and maintaining a local area network? This is not very likely. Once again, an overall Marine Corps maintenance strategy is in order. If local networks really will become an integral part of the Marine Corps' data processing and communications network strategy, then appropriate staffing and facilities improvements to existing CEO or Automated Services Center organizations should be planned. At the very least, someone (probably the CEO) should assume responsibility for an overall base cable plant improvement plan. This plan should include provisions for local area networks. Planned fiber optic cable installations like the one at Iwakuni, Japan and T1 carrier backbone systems like the one going in to support the new Northern Telecom switchboard installation at Camp Pendleton, Ca should be considered when planning procurement and installation of future LANs. At a time when everyone is looking for compensatory personnel reductions, personnel increases for LAN support will be hard to get. All the more reason to make them a part of a coordinated support strategy. This will be necessary for whatever data processing and support strategy we adopt. These decisions must then be reflected in the individual LAN procurement specifications.

4. Network Management

Many defense systems support hundreds, even thousands of users distributed around the world. USMC system designers must be aware of the specific performance status report requirements, administration, and control functions they require. These functions will be performed by a LAN control center and network operations center when directly connected to one of these networks. Interfacing to DOD networks like DDN, most likely will require status and

service access reports at least down to the switching node level. Perhaps not every LAN will need a dedicated network control center but the lowest level for a full time manned network control center (i.e. base, region) should be part of the overall network strategy discussed earlier in this chapter. Those LANs without full time centers should still be capable of collecting basic traffic and usage statistics along with the ability to report error or fault conditions to the responsible network control.

Every LAN will require administrative support to maintain a record of cable plant routes, access points, active users, authorized access levels, etc. Adding and removing stations should be possible without bringing down the entire network and without extensive disruptive routing reconfigurations. Specific procedures and responsibilities for configuration, reconfiguration, trouble reporting, restoral coordination, and all other administrative and operational day-to-day network management requirements (Figure 3.15) should be developed and accepted before the LAN specification is final. This will ensure that those responsible specify what is needed in the way of system and network support in the requirements and specification process.

5. Security

As the number of people with LAN access increases so does the information security threat. Add to this the additional threat posed by network interconnection and the need for stringent security procedures becomes obvious. To properly develop security measures or countermeasures, this threat has to be classified and evaluated. Is the threat passive where someone without proper access only monitors traffic but doesn't alter it? Is it active where he actually alters the information? Will the unauthorized access be gained by tapping the cable used to connect LAN stations

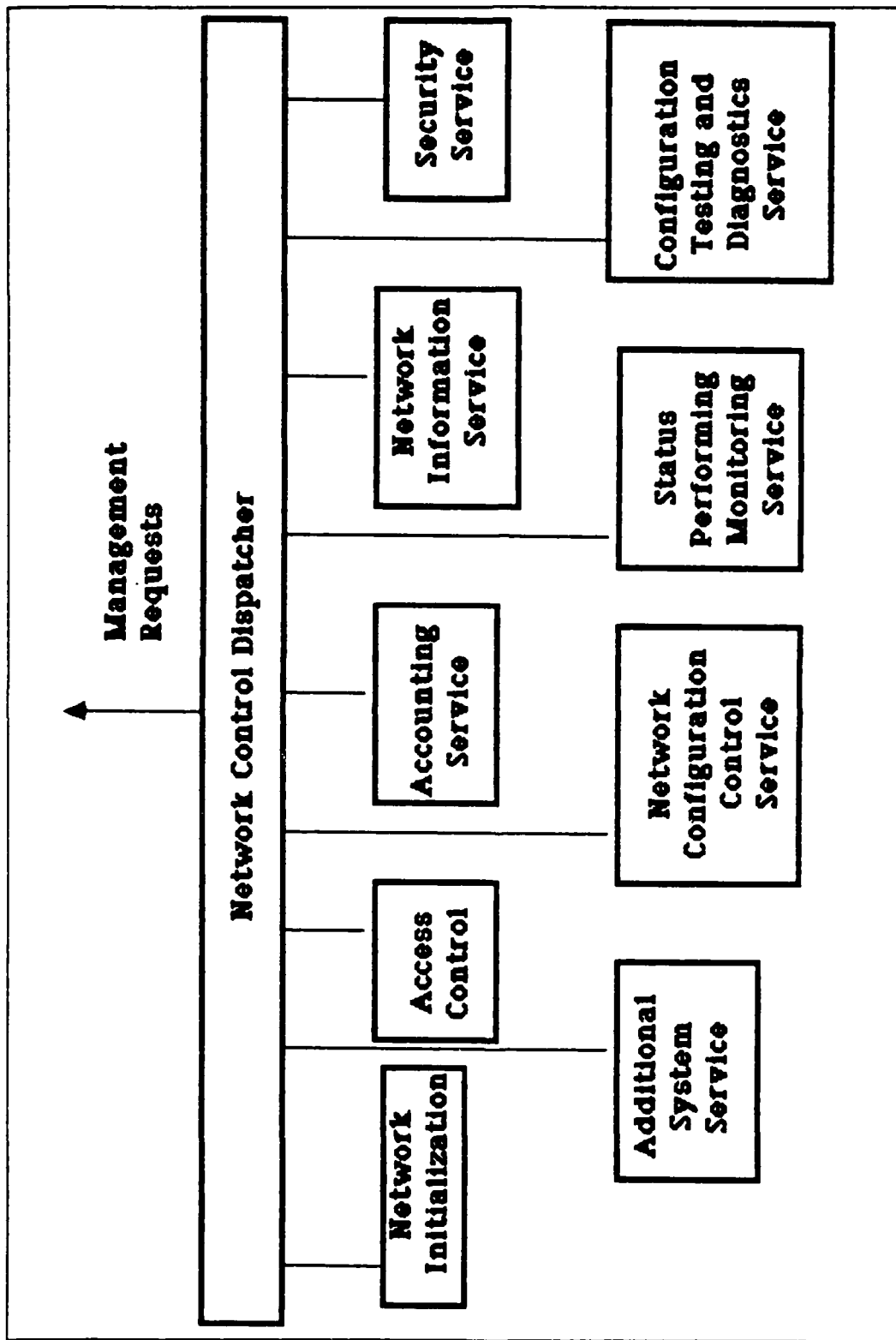


Figure 3.15 Network Management Services.

or through a bridge or gateway from a connected network? LANs (especially the bus and tree configurations) are particularly susceptible to the passive threat by their broadcast nature. Everything transmitted on the bus is received by anyone connected. Complete segregation and physical security of a special classified LAN is one answer.

Physically protecting all stations and cable plant, using a token passing ring network with a central token controller, and using approved encryption devices between the terminals and the network are all methods for improving security. In this configuration, often called the system high mode, all data processing information is treated as having the same security level - the highest level in the system [Ref. 24: p. 117]. This, however, prevents the secure network from taking advantage of the data, support, and long distances services offered by interconnection to other networks.

A great deal of work is being done on a more appropriate strategy called multilevel security. This technique allows information at various security levels as well as users with different security clearances to access and use the LAN simultaneously. This is done through a combination of end-to-end encryption of classified information and the joint use of a secure operating system, trusted software, and physical protection. DOD has tended to implement end-to-end encryption only because the addition of other methods adds cost and complexity to all of the system aspects--software, hardware, and management. A second reason is the fear that, no matter how well designed, software is still more susceptible to passive modification and tampering. NSA is currently working on the multi-level technique with a system called BLACKER. This approach, although considered by many to be more complex than some other approaches, fits well in the OSI protocol model and most likely will be the accepted system for some time [Ref. 24: p. 118].

The multilevel security approach will likely take a back seat until the technology can demonstrate sustained, accurate, economic, and adequate protection for classified material. The National Bureau of Standards has generated a great deal of interest in their work on Data Encryption Standard (DES) chips for LAN network interface units. This work includes work on the protocol layer for implementing DES ciphers, session protocols for establishing secure communications and the most important aspect, key generation and distribution. Again the fear is that the key distribution software may be secure when originally designed and produced but what prevents tampering and modification once it is fielded. Full general-purpose operating systems have so far been too complex to be totally secure so most multilevel efforts have concentrated on protecting portions of the software with trusted kernels. All security decisions are made in the trusted kernel. This requires another set of those protocol translations or mapping processes which of course degrades system performance. The true challenge for future multilevel secure system designers is security enforcement without overall system degradation [Ref. 7: pp. III-65-III-66].

Below the security classification level, non secure LANs also require certain security features to protect information being shared by many different users. The following is a list of the minimum security features that should be offered by any LAN:

- User access controls (passwords) which provide appropriate assurances each user is authorized to have access to system resources.
- Intrusion protection methods to protect against unauthorized users who may be able to break through access controls.
- Data protection and recovery techniques to permit rapid recovery of information if primary files are damaged or lost.
- Appropriate protection for a common database (like record or file locks) which permits actions (read, edit, store, etc,) dependent upon assigned code.

G. SUMMARY

LAN specifications should not be a broad, general, and basic statement of user needs added to a selected group of low-level technical and logical performance features taken from vendor advertisements. This strategy preselects LAN technology as the solution essentially eliminating other technical solutions from the beginning. A more appropriate strategy is one that adopts a system versus component approach looking from the top down rather than from the bottom up.

This strategy incorporates a detailed functional characterization of user needs and applications translated into higher-level services and, where possible, higher-level protocols. This translation is then augmented by interconnection and communications services required by these needs and applications. The up front work permits a layered system design approach which concentrates on performance and functionality for proper selection of the technology best suited to satisfy user requirements. Once a LAN is the technology selected, the addition of expected LAN oriented performance characteristics, facilities and support, network management, security, and any other needed features and constraints results in preparation of a more accurate and complete specification document for the solicitation package. This extra effort ensures vendors don't have the opportunity to submit proposals that have an abundance of detail on their individual system features without ever translating these features into operational performance capabilities. The next step in the LAN specification and selection process is development of the selection criteria used to select the vendor proposal that best suits system user, manager, and support requirements.

IV. A LAN SELECTION STRATEGY

A. GENERAL

The user and interconnection requirements augmented by the expected general performance, facilities/support, network management, security, and other feature requirements stated in the specification document should be directly translated into test objectives and test procedures then used as evaluation criteria. Various media, topologies, access methods, and other items may be appropriate for the specified environment. Hopefully, many different local networks submitted in vendor proposals will satisfy the elements of the specifications. The next question is how to correctly choose the local network or networks that will most completely satisfy the specified requirements. There is still some danger that those making the selection will revert to the general categorization of vendor offered technology and features allowing user and network specific requirements to take a back seat. This is natural because most modeling and analysis information available in recent public periodicals and government studies concentrate on this type of evaluation. The information contained in these reference sources should be used as a supplement to rather than a substitute for the specifications.

Technological variables like media, topologies, and access methods are the most popular categories used in recent literature to compare the merits of existing local area networks. The individual categories are often compared separately causing many to discard a given network because the access method or topology does not fit the required need. This is a bad practice because other features employed by the complete network design may offset the perceived system shortcoming. It appears that fashion or

technological inertia have a tendency to take over when a new solution is introduced. It is important to realize that there may be no single solution that handles the entire problem. A full solution may require multiple technologies working together. General technological comparisons along with quantitative analyses on traffic handling capabilities can give those responsible for the choice a good background in common industry standards. These comparisons also give them a feel for the performance of different networks under specified traffic loads.

The ability to build a prototype network on which actual user applications can be tried obviously offers the best assurance that a vendor's proposed network is the best solution. This however, is unrealistic because the research and development money to undertake such a task for every potential LAN requirement is simply not available. LAN specification and evaluation document preparers can however, take advantage of lessons learned from previous prototype and operational LAN network installations. Making the information available from a centrally controlled reference database would offer the prospective LAN user, designer, and manager an incredibly powerful tool for network design, specification, installation, and evaluation. Independently run tests and evaluations of actual networks provide substantial performance characteristics on protocol design and compatibility, traffic handling characteristics, geographic coverage, use and applications, surviveability, expandability, etc. Documentation of experiences that closely approximate U.S. Marine Corps user specific applications and networking requirements would offer a tremendous repository of information. It may even allow recommendation of vendor equipment configurations particularly useful in design and evaluation efforts.

Several references were reviewed as part of the research for this thesis. Some presented problems encountered and lessons learned in early prototype and operational LAN installations. Others offered comparisons of major technological variables that differentiate LAN types. Still others offered current industry trends that are likely to impact future LAN offerings. On a rare occasion, a reference was encountered that offered all of these comparisons. The point here is that although periodicals and government reports may not provide a complete set of LAN selection criteria, their use as a common information and reference tool should not be ignored. The hands on experience and actual data collection when viewed with a careful eye can add the experience factor missing in purely theoretical analysis and forecasting.

B. USER/DEVELOPER EXPERIENCE

Capitalizing on previous experience can be both a blessing and a curse. The ability to begin with knowledge and experience gained by other's mistakes prevents a great deal of lost time trying to "reinvent the wheel" and in this regard is most helpful. Unfortunately, this information also has a tendency to narrowly focus the concentration of system users, designers, and managers on only a few specific technical aspects--as stressed throughout this thesis, the danger to be avoided. Nonetheless, this information can be most helpful when added to the detailed specification requirements from Chapter 2.

A LAN prototype network test was conducted in early 1985 by the Regional Automated Services Center (RASC) at Camp Pendleton, Ca. This test was designed to determine if a local network could be used to simultaneously support personal computer networks requested by numerous Camp Pendleton User Requirement and Information Flow (URIF) studies as well as improve response times for selected 3270

terminals. The 3270 terminals were connected to MCDN through the Camp Pendleton node. After research and discussion with several potential vendors, a prototype LAN using Racal/Milago's PLANET network was installed to test the following requirements:

- Multi-point capability for devices connected to the COMTEN's
- 3270 bi-synchronous support
- PC to PC connectivity for data transfer and resource sharing
- Distributed processing support for remote locations
- PC to mainframe connectivity for data upload/download using 3270 emulation on the PCs

Additional inherent characteristics like protocol independence, redundancy, multi-point capability, plus diagnostics and remote network control from a central location were also used to select this particular LAN. The specifications concentrated heavily on technical interface requirements while not trying to predict or characterize user requirements.

It should be obvious that this test configuration assumed MCDN would be the desired long distance network and centralized host data processing would continue to be the USMC data processing strategy. This is supported by the requirement for synchronous 3270 terminals to coexist with personal computers which used 3270 emulation for host interface connection. The overall results of the test [Ref. 25: Encl 4] reinforce the ideas presented in this thesis, most notably, 1) the selection of any LAN must be done to satisfy the end user's requirements and not based solely upon technical considerations and 2) any LAN utilized by the Marine Corps should be one with full connectivity. Table X shows the recommended list of minimal specifications generated by specific test results. Recommended selection criteria like this can be used as a good source of support information for the Marine Corps networking and data processing strategy

decisions. Publication of these items alone however, will not guarantee commonalty, compatibility, or even interoperability among USMC LANs. This is especially true for those procured independently by various individual organizations. Their broad and basic nature alone opens the door to a multitude of different solutions yet the wide variety of features they demand could drive any vendor solution beyond the reasonable budget of those interested in them. This kind of test effort should be taken one step further. Once the network is operational, representative samples of user application traffic should be introduced with network connectivity as close to realistic as possible. In this manner common USMC applications needs, and perhaps standard solutions could be identified. Only tests like this will identify interface and protocol deficiencies which need to be corrected to ensure the desired connectivity and interoperability.

C. THE SINGLE SPECIFICATION APPROACH

The U.S. Air Force has been studying local networks since the early 80's. They recognized the need to create a networking architecture and set of standards for the diverse set of computers, operating systems, and applications currently in use or being developed. The result of their study efforts has been the decision to create a single program for local area network procurement. The objective of the Unified Local Area Network Architecture (ULANA) Program is to introduce standard LANs into the Air Force functional areas and bases in a unified manner. This will be done through a comprehensive set of common specifications for standard hardware and software operating system products. These products will be used for intra-base information flow among end-user devices, dedicated systems, shared systems, and gateways to other information transfer systems. The standard specifications will then be used as the contractual tools for LAN procurement and implementation.

TABLE X

RECOMMENDED LAN SPECIFICATIONS FROM MARCH 1985
RASC CAMP PENDLETON LAN TEST

1. The LAN must be protocol independent in order to support full connectivity, therefore communication between devices is dependent upon device software.
2. Minimum backbone speed should not be less than 10 mbps with the capability to select the port output speed to the user (range of 300 to 9600 bps at least).
3. Must be capable of supporting 3270 bi-synchronous communications where each controller is supported in a multi-drop configuration.
4. User must be able to communicate to the network server to request connections to 1) host systems, 2) other similar devices, and 3) servers.
5. Expected data traffic which must be supported:
 - a) Synchronous short bursty messages
 - b) Synchronous long regular messages (file transfers between PCs and PC to host)
 - c) Asynchronous file transfers between PCs
 - d) Both intelligent and non-intelligent devices
 - e) Bi-synchronous and SDLC protocols
 - f) 2780 RJE file transfers
6. Minimal supported devices is 500 where a supportable device could be a terminal controller with up to 32 devices.
7. Minimal distance between devices is 2000 feet to avoid signal regeneration without having a device in place.
8. LAN should be capable of supporting a minimum of 4 miles of cable plant.
9. Additions to the network should be possible without disrupting service to other users.
10. LAN must be user friendly in that a minimum of two to three simple commands are required to establish a connection to another device. This implies some type of network server capabilities inherent to the LAN.

TABLE X

RECOMMENDED LAN SPECIFICATIONS FROM MARCH 1985
RASC CAMP PENDLETON LAN TEST (cont)

11. LAN must have inherent intelligent bridges which allow for inter-LAN communication. Also, capabilities should exist which allow for inter-Network communication across the COMTEN. This requirement will require a Marine Corps wide adoption of a bridging standard.
12. The following minimal diagnostic capabilities must exist:
 - a) Fault detection - LAN must recognize when a cable, access equipment, or attached device has failed. This information must be provided at a central location.
 - b) Fault isolation - capabilities must exist to allow a technician to narrow down problem determination to the failing component or area.
 - c) Network degradation - capabilities must exist to monitor LAN performance in terms of backbone speed and access port speeds.
13. LAN must be capable of establishing virtual circuit connections between devices. This feature is a given for almost all LANs, but re-stating can not hurt.
14. Must be capable of operating off standard house current.
15. Vendor should be able to provide the following:
 - a) Training - on site training for teleprocessing technicians and software programmers. Minimum of two days of assistance and instruction.
 - b) Maintenance - capable of responding to a trouble call within two hours and sufficient repair parts available to effect repairs within one day.
 - c) Delivery - capable of delivering equipment within 60 days of receipt of purchase order and equipment must be off the shelf.
16. LAN must be capable of switching at the device level. This capability must be able to be overridden from a central control location (i.e. Network Control).
17. Access security at the device level must be at least three stages. In other words, central control can limit what switching/access capabilities each user has (i.e. between LANs, to servers, speed, type of protocol, etc.).
18. Capable of sustaining a single failure without disrupting the entire network.

The following is the list of these tools:

- Standard System Specification - rules governing the overall architecture and functioning of the network
- Standard Cable Plant Design Specification - performance, monitoring, and maintenance standard for a common transmission media (broadband with options for twisted pair and fiber optics)
- Prototype CAD/CAE Station - a prototype system for engineering and designing dual coaxial broadband cable plants for LANs using computer aided design/computer aided engineering technologies
- Standard Network Interface and Interconnects Units - a family of hardware/software devices that allows the subscribers to connect various information processing (subscriber devices) to the network
- Standard Network Management System - the ULANA networks operational, supervisory, and control hardware and software
- ULANA Management System (UMS) - an Air Force centralized system which provides data to Air Force Personnel regarding LAN user requirements, operations, performance, maintenance, and other management functions.

If realized, the ULANA network standard network interface units, cable plants, bridges, gateways, plus operational, supervisory, and control software will permit the interconnection of a variety of diverse electronic devices. Mainframe computers, minicomputers, microcomputers, terminals, printers, television cameras, television receivers, telephones, and sensing equipment will be connected through five different communications subnets. Figure 4.1 shows the frequency assignments that will allow data, host, control, switched, and video subnets to share the broadband frequency range. The data services will use both a fixed frequency band (138-174 MHZ) and a frequency selectable band (216-312 MHZ). Switched voice and video service requirements will use 312-348 MHZ. All of this will be done on a cable that is also capable of simultaneously handling the standard FM voice band and public television broadcast video channels if desired. The Broadband cable plant uses a common segmented tree topology with dual coaxial cables connected through multiple redundant headend devices for building and base connectivity (Figure 4.2).

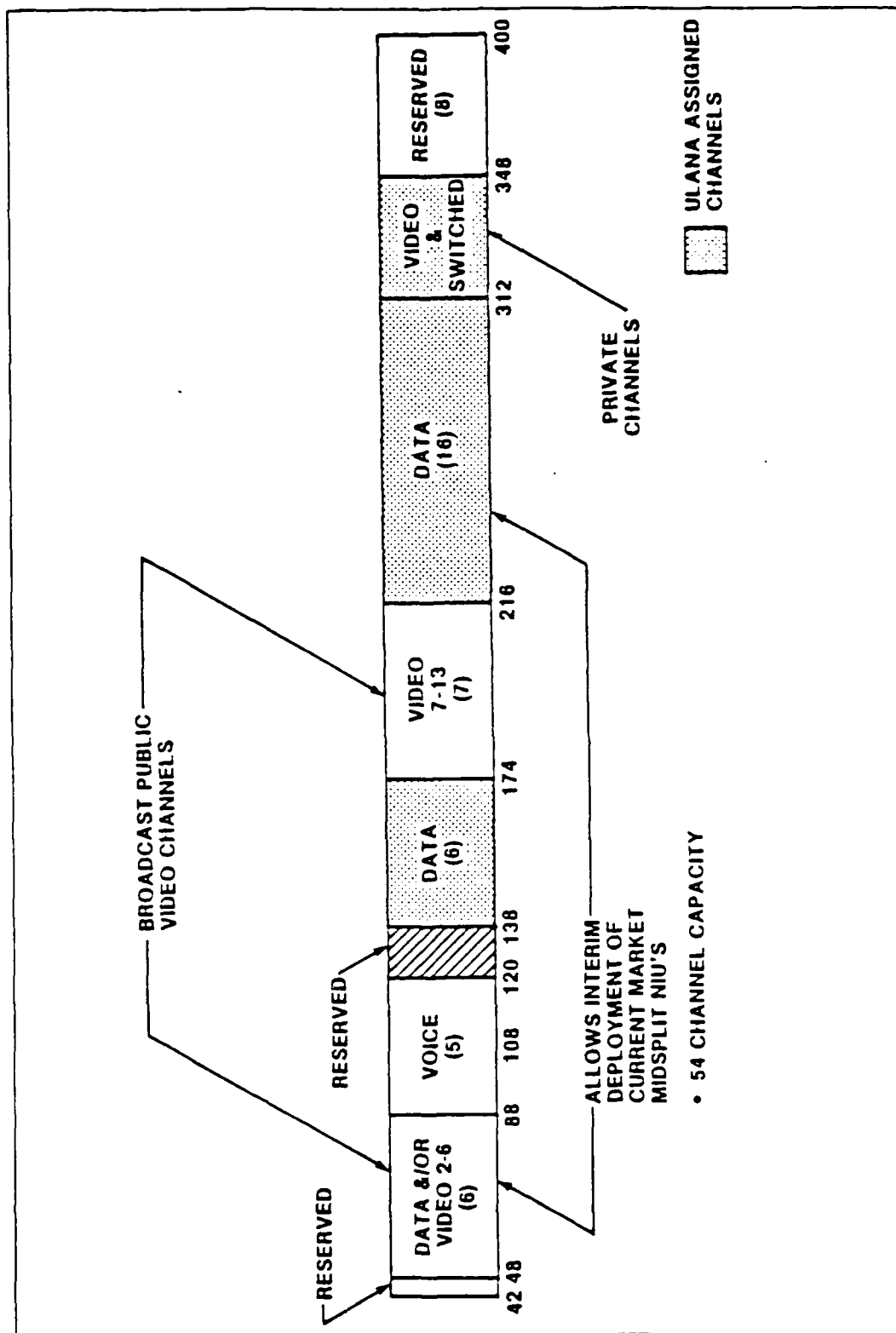


Figure 4.1 ULANA Frequency Allocation.

This is a far sighted local area communications system architecture. It allows simultaneous interconnection of a wide variety of user applications. It also offers the ability to transition to a smaller number of subnets should any of these applications be able to use common transmission techniques and protocols in the future.

Regardless of whether the U.S. Marine Corps elects to publish a common set of specifications and selection criteria or a common set of standards and guidelines, the more hardware and software parts of the system that can be standardized, the better the chances for interoperability as well as economic support. No one solution may suit all situations, but augmenting user specific requirements with other's prototype experiences will help select the best solution. Independent network analysis tests and results will also decrease the chance of selecting a network that does not meet the specified requirements.

V. SUMMARY/CONCLUSIONS

The emergence of the microcomputer as a powerful personal productivity tool was probably most instrumental in the move away from large costly, centralized mainframe processing systems. Better accessibility, greater interaction, and a wider choice of equipment are all advantages of the new personal computer (PC) technology. However, problems like expensive peripherals, lack of data file integrity from one station to another, inability to easily share information, and database/program maintenance have driven users and network designers toward the search for cost effective ways to link these disparate information processing and storage tools. Local area networks (LANs) are fast becoming the logical evolutionary step in development of a shared multi-user network to satisfy this connectivity requirement.

LAN vendors offer a wide variety of topologies, control structures, media, access control techniques, and other items designed to satisfy individual needs. They offer the potential for more flexible connectivity among processors, workstations, storage devices, and expensive peripherals in the local area. These features are offered at greater speeds and lower cost than possible in the previous host-dependent data processing environment. None, however, have come up with a design that looks like it will become the standard or clear cut solution to everyone's needs. This has caused a great deal of confusion on the part of prospective buyers. It has also resulted in procurement and installation of many heterogeneous networks that cannot support the same kind of equipment or cannot intercommunicate.

Independent individual procurement was an acceptable strategy for PCs because their cost was not particularly high. Organizations basically used them to improve productivity within their own span of control having little or no affect on others. LAN networks require costly special cables, interface devices, and sophisticated servers. These costs along with individually purchased maintenance and support contracts are rapidly off-setting the advantages of low cost, intelligent, individual workstations over the traditional mainframe approach.

The lack of official guidance along with inflated vendor claims have created groups of "system hunters" who develop broad or superficial user requirements. They then compare and evaluate the capabilities of existing hardware and software solutions to satisfy these requirements. A thorough definition of user needs is never accomplished. This bottom up approach, using broad general user requirement specifications and lower-level technical considerations, just gives the vendor an opportunity to submit an abundance of detail on the features of his own system. He never translates those features into required operational performance capabilities. The network is essentially specified by the vendor's description of what it could do vice the user's detailed description of what was needed. These networks have few problems passing operational acceptance criteria. It is only after network installation and acceptance that the supported organizations discover other issues which should have been resolved prior to or during the LAN specification/selection process. The specification and selection of these networks deserves more detailed consideration and guidance than broadly specified user requirements augmented by technical specifications detailing vendor strategies that already exist.

A more appropriate strategy is one that adopts a system versus component approach looking at things from the top down rather than the bottom up. A close partnership between users and information system professionals is essential. You need to characterize the applications or end user requirements to be supported, the local/long distance interconnection and communications services required by user applications, and the technology available to support these requirements in that order.

The characterization of user requirements should be done first from a functional not necessarily technical standpoint. Obviously technical terms are often necessary to describe the application, but emphasis should be on the need first not the solution. Mistakenly, people often say they have a requirement for a LAN. A LAN is not a requirement but rather one element in a list of potential solutions for satisfying an information processing and transfer requirement. Information processing and transfer requirements must be characterized through analysis of prospective user mission and mission functional/subfunctional responsibilities in the lowest detail possible. The analysis of current organizational and operational management information structures, sources, and data flow techniques used to handle these mission functions is then added. This facilitates identification of deficiencies as well as connectivity and processing capabilities that already exist.

A new emphasis is needed to ensure users understand their own needs well enough to completely and accurately define them for network designers. This emphasis also gives them the opportunity to better understand the existing information management system. A poorly designed and managed information system is just as big a contributor to problems as isolated information processing and standalone PCs. As individuals or parts of the organization become

more productive, it affects everyone else whose work is connected to them. Adequate planning and preparation is essential to address changes in work responsibilities and behavior patterns, accommodate user concerns, and allow smooth transition to new capabilities. Moving information between user applications without labor intensive intermediate handling or reformatting in a manner that supports the way people really work and think will be the key to success.

The identity of individual subfunctions must be preserved for future development of specifications as well as test and evaluation criteria. These functions can however, be grouped in common applications and higher-level services. Various information systems use application processes or logical elements called protocols to perform the services required by specific user applications. The exchange of information among data transfer systems is a complicated process. The required cooperation must be formalized in rules which define the methods, procedures, and conventions needed to complete the information exchange. Standards at the network layer and above are critical for compatibility and communications LAN to LAN and LAN to WAN. USMC programmers and engineers will not likely write protocols that support user applications or communications interfaces. However, we should develop a method to evaluate where specific protocol services fit within the general OSI/RM and whether they fit our needs. The keen competition for diminishing research, development, production and operating funds almost mandates procurement of existing off-the-shelf network and processing components to reduce development costs and allow economic logistics and maintenance support. This should not however, reduce our efforts to properly define our actual requirements to ensure we get a system that meets our needs yet does not have expensive unnecessary features accepted just because they were available.

As local network capabilities grow, so will the desire to expand the geographic coverage of the systems providing these capabilities. This will increase the need for both local and long distance LAN interconnection. If not adequately addressed in the planning stages of LAN design, the result will be efficient pockets of high speed data processing and data communication systems that are seriously degraded by inefficient interconnection solutions. There are many different established long distance network protocols (INTERNET, SNA, DNA, etc). The Marine Corps should develop an overall data processing and long distance network interconnection strategy. This will ensure that unnecessary expensive connection, bridges, gateways, and protocol conversion requirements are not imposed on all LAN specifications just to cover all the contingencies. Will data processing continue to be the centralized host oriented operation it is today or will a more distributed operation be adopted in the future? Will DDN, MCDN, PSNs, or a combination of all three be used for long distance interconnection? Since most LAN traffic is local, these parameters may not be the driving force in LAN access and communication strategies but they cannot be ignored. This reduces the chance of selecting a LAN that is rendered woefully inefficient or even worse cannot pass traffic when connected to a long distance network.

Once a LAN is the technology selected, expected LAN oriented performance characteristics, facilities and support, network management, security and any other needed features/constraints should be added. This results in preparation of a more accurate and complete specification document for the solicitation package. Modular design techniques will ensure that the entire system does not require replacement all at once. Commercially available parts and software tools reduce supportability costs.

Contractual flexibility is the key to substituting modern components during the life of the contract. Technology should be used to reduce manpower intensive operations. Simply substituting newer versions of existing physical systems or even worse adding additional systems is not the solution.

Who will provide the day-to-day maintenance and network control support for LANs? Once again an overall Marine Corps maintenance strategy is in needed. If local networks really will become an integral part of the Marine Corps' data processing and communications network strategy, then appropriate staffing and facilities improvements to existing organizations must be planned. Perhaps not every LAN will need a dedicated network control center, but the lowest level with a full time manned center should be identified and subordinate network administrative, maintenance, and operational responsibilities should be formalized.

The specified requirements should be directly translated into evaluation criteria for selecting from the various vendor proposals. No one solution may suit all situations. However, augmenting user specific requirements with other's prototype experiences as well as independent network analysis and test results will decrease the chance of selecting a network that does not meet specified requirements

Execution of all the steps and procedures addressed in this thesis for each and every LAN procurement would be very costly in terms of time and money. A centrally controlled database should be created to act as a repository of information for prospective LAN users, designers, and procurement specialists. This could greatly reduce the research and analysis effort required. Those with like or identical requirements to existent prototype or operational LANs could take advantage of lessons learned, problems solved, and tried and tested procedures and specifications. This

database could also be used by those responsible for developing an overall USMC data processing and communication network strategies. They would have the opportunity to catalog and consider the many user applications and connectivity requirements to be satisfied by these strategies. Because no single vendor has demonstrated the ability to take a lead in LAN technology, it would be wise to limit LAN network development and investment to low cost prototype networks. Once the database is mature enough and the LAN competition settles down to a few clear leaders, prudent LAN investment decisions will be possible.

APPENDIX

ACRONYMS

AFB - Air Force Base

AIS - Automated Information System

BPS - Bits per second

CAD - Computer Aided Design

CAE - Computer Aide Engineering

CATV - Community Antenna Television

CBX - Computerized Branch Exchange

CCITT - International Telegraph and Telephone Consultive
Committee

CD - Collision Detection

CEO - Communication Electronics Officer

CPU - Central Processing Unit

CSMA - Carrier Sense Multiple Access

DCA - Defense Communications Agency

DCE - Digital Circuit Switching Equipment

DDCMP - Digital Data Communications Message Protocol

DDN - Defense Data Network

DEC - Digital Equipment Corporation

DES - Data Encryption Standard

DNA - Digital Network Architecture

DOD - Department of Defense

DTE - Digital Terminal Equipment
FEP - Front End Processor
FM - Frequency Modulation
FTAM - File Transfer Access and Management
IEEE - Institute of Electrical and Electronic Engineers
IP - Internet Protocol
ISO - International Standards Organization
KBPS - Kilobits per second
KHZ - Kiloohertz
LAN - Local Area Network
MBPS - Megabits per second
MCDN - Marine Corps Data Network
MHZ - Megahertz
NAU - Network Addressable Unit
NSA - National Security Agency
NSP - Network Services Protocol
OSI - Open System Interconnection
PABX - Private Automatic Branch Exchange
PBX - Private Branch Exchange
PC - Personal Computer
PCM - Pulse Code Modulation
PSN - Public Switched Network
RASC - Regional Automated Services Center

RJE - Remote Job Entry
RM - Reference Model
SDLC - Synchronous Data Link Control
SSCP - System Services Control Point
TCP - Transmission Control Protocol
TDM - Time Division Multiplexing
TDMA - Time Division Multiple Access
ULANA - Unified Local Area Network Architecture
UMS - ULANA Management System
URIF - User Requirement Information
WAN - Wide Area Network

LIST OF REFERENCES

1. Wells, J.D., IBM's Token-Ring LAN (Local Area Network) A Base-Level Communications Solution, Student Report, Air Command and Staff College, Maxwell AFB, April, 1984.
2. Information Processing, "Linking Office Computers: The Market Comes of Age", Businessweek, May 14, 1984.
3. Thurber, Kenneth J., "Local Network Selection Criteria", Proceedings of LOCAL NET84, San Diego, Ca, October 1984.
4. Elden, Walter L. et al, LAN (Local Area Network) Interoperability Study of Protocols Needed for Distributed Command and Control, Harris Corp. Study, March 1985.
5. Schneidwind, Norman F., "Interconnecting Local Networks to Long Distance Networks", Computer, IEEE Computer Society, Vol 16, No 9, September 1983.
6. Yeh, J. et al, Local Area Networking Technology Survey, Integrated System Inc. Report, Rockville, Md, February 1982.
7. Yeh, J. et al, Local Area Network: Technology Products and Trends Volume 3 Assessments, Integrated Microcomputer Systems Inc. Report, Rockville, Md., January 1984.
8. Stallings, William, Local Networks An Introduction, Macmillan, New York, 1984.
9. Zimmerman, Hubert, "OSI Reference Model - The ISO Model Architecture for Open Systems Interconnection", IEEE Transactions on Communications, Vol. Com28, No 4, April 1980.
10. Conard, James W., "Character-Oriented Data Link Control Protocols", IEEE Transactions on Communications, Vol. Com28, No 4, April 1980.
11. Houldsworth, Jack, "Convergence of LAN and Digital Telephone Exchange Systems", Proceedings of LOCAL NET83, London, UK, March 1983.
12. McDonnell, Jerry, "Broadband or baseband: CSMA/CD or Token - What's the Difference?", Proceedings, LOCAL NET84, San Diego, Ca, October 1984.

13. Roelandts, Wim, "Trudging Through the Interconnect Maze: A Field Guide", Data Communications, May 1985.
14. Jewett, Roger F., "The Fourth-Generation PBX - Beyond the Integration of Voice and Data", Telecommunications, February 1985.
15. Feltman, Charles, "Personal Computers & Organizational Productivity", Proceedings, LOCAL NET84, San Diego, Ca., October 1984.
16. Lewan, Douglas and H. Garrett Long, "The OSI File Service", Proceeding of IEEE, Vol 71, No 12, December 1983.
17. Sproull, Robert F. and Dan Cohen, "High-Level Protocols", Proceedings of the IEEE, Vol 66, No 11, November 1978.
18. Bartoli, Paul D., "The application and Presentation Layers of the Reference Model for Open Systems Interconnection", Proceeding of INFOCOM 83, San Diego, Ca., May 1983.
19. Bowers, Albert W., "A Checklist of Communications Protocol Functions Organized Using the Open System Interconnection Model", Proceedings of COMPCON F'83, Arlington, Va., September 1983.
20. Stallings, William, Data and Computer Communications, Macmillan, New York, 1985.
21. Warner, Clifford, "Connecting Local Networks to Long Haul Networks: Issues in Protocol Design", Local Network Technology Tutorial, IEEE Catalog Number EH0234-5, IEEE Computer Society Press, Washington, D.C., 1983.
22. Stallings, William, "Beyond Local Networks", Datamation, August 1983.
23. Flint, David, "The selection of a Local Communications Network", Proceeding of LOCAL NET83, London, UK, March 1983.
24. Omidyar, Dr C. Guy, and Mohan K. Malhotra, "Trends and Issues in Local Area Networks", Proceedings of the Fiber Optic Communications and Local Area Networks Exposition, September 1984.
25. Commanding General, Marine Corps Base Camp Pendleton, Ca letter 5230-40, BG/WTG/mef, Local Area Networks, Study Results, 25 March 1985.

INITIAL DISTRIBUTION LIST

	No.	Copies
1. Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145		2
2. Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002		2
3. Major Timothy J. Himes Headquarters, U.S. Marine Corps Code LMC-1 Washington, D.C. 20380-0001		5
4. Commandant of the Marine Corps (Code CCTO) Headquarters, U.S. Marine Corps Washington, D.C. 20380-0001		3
5. Regional Automated Service Center (Attn. Capt W.T. Greer) Marine Corps Base Camp Pendleton, Ca 92055-5000		1
6. Professor Jack W. LaPatra Code 54LP Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000		1
7. Major Thomas J. Brown Code-39 C3 Academic Group Naval Postgraduate School Monterey, California 93943-5000		1
8. Professor Carl R. Jones Code 54JS Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000		1
9. Mr. Ken Boheim NCS/PP 8th St. & S. Courthouse Arlington, Va. 22204		1
10. Mr. Edward M. Cain NCS/PP 8th St. & S. Courthouse Arlington, Va. 22204		1
11. Dr. Bruce Barrow NCS/PP 8th St. & S. Courthouse Arlington, Va. 22204		1
12. Col William Schooler NCS-EP 8th St. & S. Courthouse Arlington, Va. 22204		1

- | | | |
|-----|-------------------------------|---|
| 13. | Mr. Norman Douglas | 1 |
| | NCS-EP | |
| | 8th St. & S. Courthouse | |
| | Arlington, Va. 22204 | |
| 14. | LTC Tom Cindrie (JDSSC) | 1 |
| | Defense Communications Agency | |
| | Code 662 | |
| | Washington, D.C. 20305 | |

END

DTIC

8-86